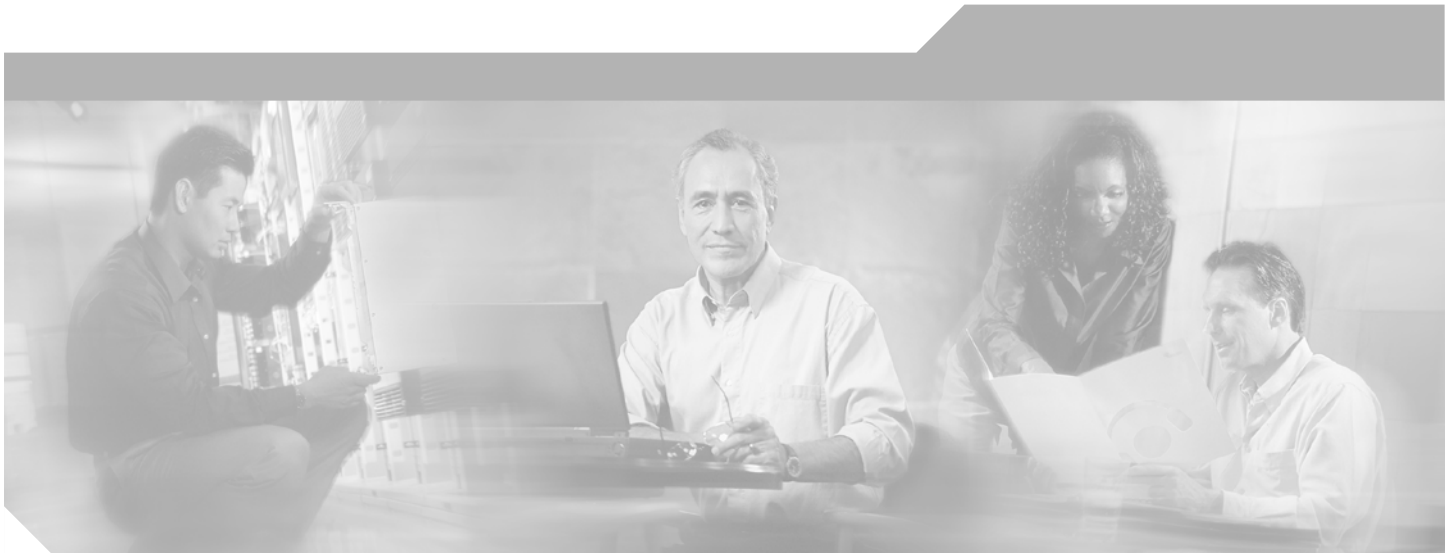


Cisco Aironet 1300 Series Wireless Outdoor Access Point/Bridge Hardware Installation Guide

December 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5048-06

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Aironet 1300 Series Wireless Outdoor Access Point/Bridge Hardware Installation Guide

CONTENTS

Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1300 Series Outdoor Access Point/Bridge. The 1300 series access point/bridge is available in autonomous and lightweight configurations.

To use this guide with an autonomous access point/bridge, you should have experience working with Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

To use this guide with lightweight access points, you should have experience working with a Cisco wireless LAN controller (hereafter called a *controller*) and be familiar with the concepts and terminology of wireless LANs.

Purpose

This guide provides the information you need to install your autonomous or lightweight access point.

For detailed information about Cisco IOS commands used with autonomous access points, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS Release 12.3 commands, refer to the Cisco IOS documentation set available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Cisco IOS Software > Cisco IOS Software Releases 12.3 Mainline**.

For information about controllers, refer to the Cisco documentation sets available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Wireless** and the documentation is listed under the "Wireless LAN Controllers" section.

Organization

This guide contains the following sections:

Chapter 1, "Overview," describes the major components, features, and specifications of the access point/bridge.

Chapter 2, "Installation Overview," provides warnings, safety information, and information needed before you begin the installation of your access point/bridge system.

Chapter 3, "Mounting Overview," provides an overview of components and features used during access point/bridge mounting and antenna alignment operations.

Chapter 4, "Troubleshooting Autonomous Access Points and Bridges," provides solutions to potential problems encountered during setup of autonomous access points.

Chapter 5, "Troubleshooting Lightweight Access Points," provides solutions to potential problems encountered during setup of lightweightaccess points.

Appendix A, "Translated Safety Warnings," indicates how to access the document that provides translations of the safety warnings that appear in this publication.

Appendix B, "Declarations of Conformity and Regulatory Information," describes the regulatory conventions to which the access point/bridge conforms and provides guidelines for operating access point/bridges in Japan.

Appendix C, "Access Point Specifications," describes the channels and antenna settings supported by the regulatory organizations.

Appendix D, "Channels and Maximum Power Levels," indicates how to access the document that lists the access point/bridge radio channels and the maximum power levels supported by the world's regulatory domains.

Appendix E, "Console Serial Cable Pinouts," identifies the pinouts for the serial cable that connects to the power injector's console serial port.

Appendix F, "Priming Lightweight Access Points Prior to Deployment," describes the procedure to prime lightweight access points with controller information.

Appendix G, "Configuring DHCP Option 43 for Lightweight Access Points," describes the procedure to configure DHCP Option 43 for lightweight access points.

Appendix H, "Load-Dump Protection for Transportation Vehicles," describes load-dump protection that is required for autonomous access point/bridge operation in some transportation vehicles

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

For more information about autonomous access point/bridges and related products, refer to the following publications:

- *Cisco IOS Software Configuration Guide for Access Points*
- *Cisco Aironet 1300 Series Outdoor Bridge Mounting Instructions*
- *Release Notes for Cisco Aironet Access Points*

For more information about lightweight access point/bridges and related products, refer to the following publications:

- *Quick Start Guide: Cisco Aironet Lightweight Access Points*
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Aironet 1300 Series Lightweight Outdoor Access Point Mounting Instructions*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

Click this link to browse to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1300 series access point documentation, click **Cisco Aironet 1300 Series** listed under "Wireless LAN Access."

To browse to controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2000 Series Wireless LAN Controllers** listed under "Wireless LAN Controllers."

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

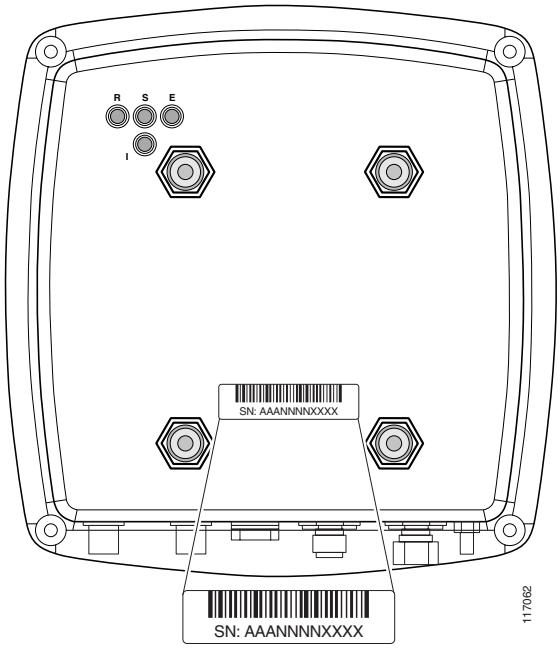
To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Locating the Product Serial Number

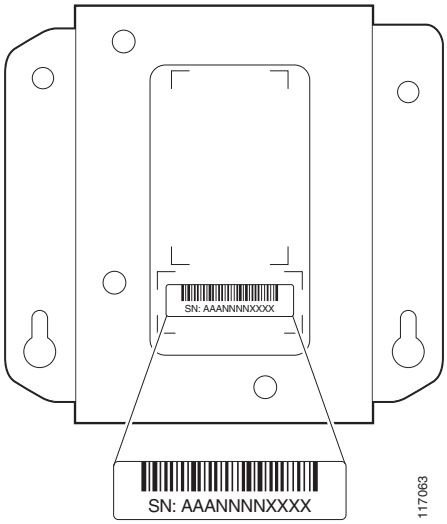
The access point/bridge serial number is located on the bottom of the cabinet (refer to Figure 1).

Figure 1 Location of Access Point Serial Number Label



The power injector serial number is located on the bottom of the cabinet (refer to Figure 2).

Figure 2 Location of Power Injector Serial Number Label



The access point/bridge serial number label contains the following information:

- Model number, such as *AIR-BR1300* or *AIR-LAP1300*
- Serial number, such as *S/N: VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as *MAC: 00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

You need your product serial number when requesting support from the Cisco Technical Assistance Center.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

The Cisco Aironet 1300 Series Outdoor Access Point/Bridge is available in autonomous and lightweight products. The autonomous product can support standalone network configurations with all configuration settings maintained within the unit. The autonomous product can be configured for multiple operating roles such as, access point, bridge, and workgroup bridge. The lightweight product operates in conjunction with a Cisco wireless LAN controller with all configuration information maintained within the controller. The lightweight product can be only configured as an access point.

Product Terminology

The following terms refer to the autonomous and lightweight products:

- The term *access point/bridge* describes both autonomous and lightweight products.
- The term *autonomous access point/bridge* describes only the autonomous product.
- The term *lightweight access point* describs only the lightweight product.
- The term *access point* describes the product when configured to operate as an access point.
- The term *bridge* describes the product when configured to operate as a bridge.

Autonomous Access Point/Bridge

The autonomous access point/bridge (model: AIR-BR1310G) supports a management system based on Cisco IOS software. The access point/bridge is a Wi-Fi certified, wireless LAN transceiver. The autonomous access point/bridge uses a single mini-PCI radio (IEEE 802.11b-compliant or IEEE 802.11g-compliant) that can be upgraded to future radio technologies.

The autonomous access point/bridge serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining uninterrupted access to the network.

You can configure and monitor the autonomous access point/bridge using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Lightweight Access Point

The lightweight access point (model: AIR-LAP1310G) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before they are mounted. The lightweight access point is automatically configured by a Cisco wreless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The lightweight access points contain one integrated radio: a 2.4-GHz radio (IEEE 802.11g). Using a controller, you can configure the radio settings.

In the Cisco Centralized Wireless LAN architecture, access points operate in the lightweight mode (as opposed to autonomous mode). The lightweight access points associate to a controller. The controller manages the configuration, firmware, and controls transactions such as 802.1x authentication. In addition, all wireless traffic is tunneled through the controller.

LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run-time operations. LWAPP also defines the tunneling mechanism for data traffic.

In an LWAPP environment, a lightweight access point discovers a controller by using LWAPP discovery mechanisms and then sends it an LWAPP join request. The controller sends the lightweight access point an LWAPP join response allowing the access point to associate with the controller. When the lightweight access point is associated, it downloads its software if the versions on the lightweight access point and controller do not match. After a lightweight access point associates with a controller, you can reassign it to any controller on your network.

LWAPP secures the control communication between the lightweight access point and controller by means of a secure key distribution, using X.509 certificates on both the lightweight access point and controller.

This chapter provides information on the following topics:

- Key Features, page 1-3
- Network Examples with Autonomous Access Point/Bridges, page 1-9
- Network Examples with Lightweight Access Points, page 1-13

Guidelines for Using a Lightweight Access Point/Bridge

You should keep these guidelines in mind when you use a lightweight access point/bridge:

- A lightweight access points/bridge can communicate only with Cisco 2006 series wireless LAN controllers or 4400 series controllers. Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because they lack the memory required to support access points running Cisco IOS software.
- A lightweight access points/bridge does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- A lightweight access points/bridge supports eight BSSIDs per radio and a total of eight wireless LANs per access point. When a lightweight access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- A lightweight access points/bridge does not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The lightweight access point console port is enabled for monitoring and debuging purposes (all configuration commands are disabled when the access point is associated to a controller).

Key Features

Key features of the access point/bridge:

- Unlicensed IEEE 802.11g 2.4-GHz radio operation
- Enclosure supports indoor or outdoor installations
- Dual-coax 100-Mbps Ethernet ports
- Four LEDs
- Inline power over dual-coax cables
- Console serial interface on power injector
- Integrated antenna or external antenna configurations (see Figure 1-1)

The autonomous access point/bridge supports these additional key features:

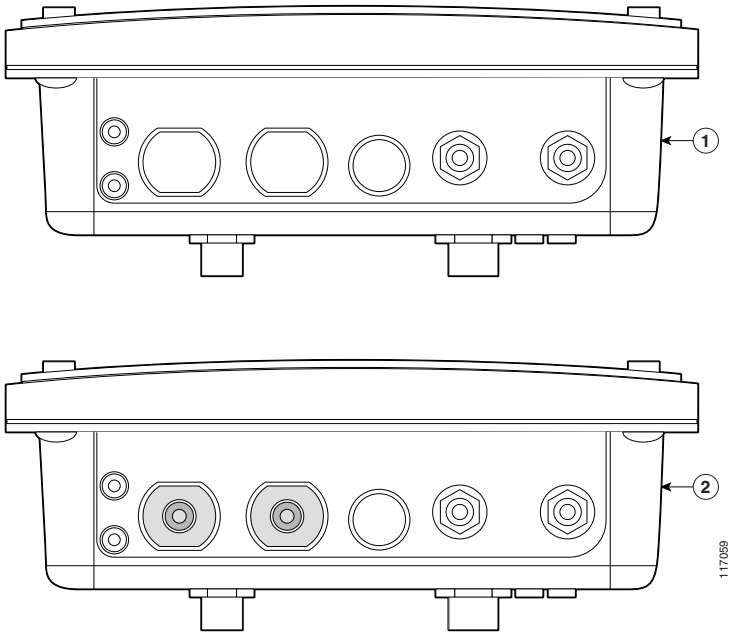
- Receive Signal Strength Indicator (RSSI) LED patterns for easy antenna alignment
- Control using Cisco IOS commands, Internet browser, SNMP, or serial interface
- Operating modes:
  - Root and non-root bridge
  - Access point
  - Workgroup bridge
  - Automatic install modes

The lightweight access point supports these additional key features:

- Centralized control using a controller
- Access point operating mode

Figure 1-1 shows the two outdoor access point/bridge configurations.

Figure 1-1 Access Point Configurations



1	Integrated antenna access point/bridge configuration	**2**	External antenna access point/bridge configuration with external antenna connectors

Note Antenna connectors are available only on the external antenna access point/bridge configuration.

Note The external antenna access point/bridge configuration does not ship with an external antenna. An external antenna must be purchased.

Power

The access point/bridge receives inline power from the Cisco Aironet Power Injector (hereafter called the *power injector*). Dual-coax cables are used to provide Ethernet data and power from the power injector to the access point/bridge. The power injector is an external unit designed for operation in a sheltered environment, such as inside a building or vehicle. The power injector also functions as an Ethernet repeater by connecting to a Category 5 LAN backbone and using the dual-coax cable interface to the access point/bridge.

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the access point/bridge)
  - 48-VDC input power
  - Uses the 48-VDC power module (included with the access point/bridge)

- Cisco Aironet Power Injector LR2T—optional transportation version
  - 12- to 40-VDC input power

Note The power injector and the power module must not be placed in an outdoor unprotected environment. The power module must not be placed in a building's environmental air space, such as above a suspended ceiling.

Integrated Antenna

The access point/bridge is available with an integrated 13-dBi patch array antenna. The antenna is covered with a radome to protect it from environmental elements. The integrated antenna is vertically polarized.

Note Some international regulatory regions may restrict the integrated antenna access point/bridge configuration.

External Antenna

The access point/bridge is available in an external antenna configuration (see Figure 1-1) for use with Cisco Aironet 2.4-GHz antennas. Two reverse-TNC type RF connectors are provided on the end of the unit to support single or diversity antenna configurations. The antennas connect to the access point/bridge antenna connectors using a coax cable. Table 1-1 lists the external antennas supported by the access point/bridge.

Table 1-1 Supported External Antennas

Antenna	Description
AIR-ANT2506	5.2-dBi omnidirectional antenna with vertical polarization
AIR-ANT3549	9-dBi patch wall mount antenna
AIR-ANT2410Y-R	10-dBi yagi antenna
AIR-ANT24120[1]	12-dBi omnidirectional antenna with vertical polarization
AIR-ANT1949[1]	13.5-dBi yagi antenna
AIR-ANT2414S-R[1]	14-dBi sector antenna with vertical polarization
AIR-ANT3338[1]	21-dBi dish antenna

1. Not supported by the lightweight access point (AIR-LAP1310G)

Note To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administrator or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Ethernet Ports

The access point/bridge dual-coax Ethernet ports consists of a pair of 75-ohm F-type connectors, linking the unit to your 100BASE-T Ethernet LAN through the power injector. The dual-coax cables are used to send and receive Ethernet data and to supply inline 48-VDC power from the power injector to the access point/bridge. For the location of the ports, refer to Figure 1-3.

Enclosure

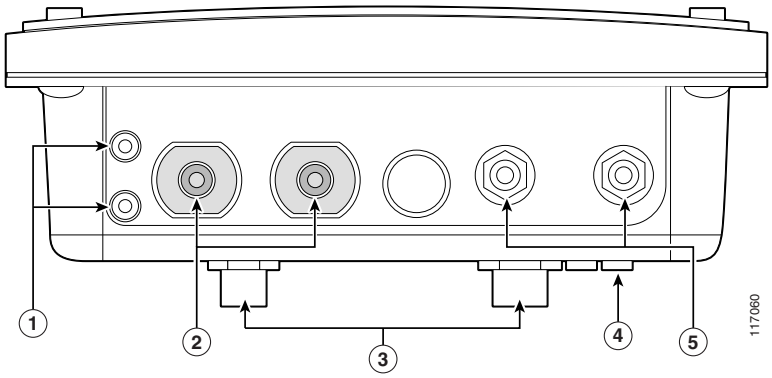
The access point/bridge uses an enclosure that supports indoor or outdoor operating environments. (refer to "Access Point Specifications" section on page C-1).

Connectors

The connectors (see Figure 1-2) provided depend upon the access point/bridge configuration:

- Integrated antenna access point/bridge configuration
  - Dual-coax Ethernet connectors—used to provide Ethernet signals and in-line power
- External antenna access point/bridge configuration
  - Dual-coax Ethernet connectors—used to provide Ethernet signals and in-line power
  - Dual antenna connectors—used to support a single antenna or dual-diversity antennas

Figure 1-2 Access Point Connector Locations

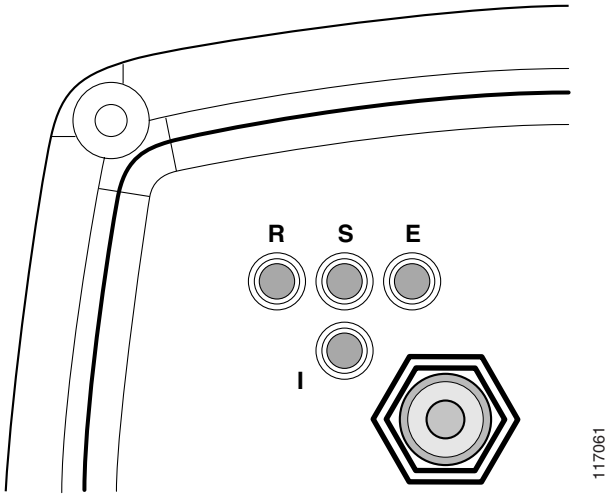


1	Ground lug mounting screws	**3**	Mounting posts
2	Left antenna connector (external antenna access point/bridge configuration only)	**4**	LEDs
	Primary right antenna connector (external antenna access point/bridge configuration only)	**5**	Dual-coax Ethernet ports (F-Type connectors)

LEDs

Four LEDs are located on back of the housing to report radio activity, status, and Ethernet activity (see Figure 1-3).

Figure 1-3 LEDs



R	Radio LED (R)	**E**	Ethernet LED (E)
S	Status LED (S)	**I**	Install LED (I)

- The install LED indicates that installation mode is activated. During installation mode, the other LEDs provide signal strength readings used for antenna alignment.

Note The install LED is not used on the lightweight access points.

- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the radio link. This LED also provides signal strength readings during installation mode. On autonomous access points, this LED also provides signal strength readings during installation mode.
- The status LED indicates association status. Blinking green indicates that the access point/bridge is not associated with another bridge. Steady green indicates that the unit is associated with at least one other bridge. On autonomous access points, this LED also provides signal strength readings during installation mode.
- The Ethernet LED indicates Ethernet traffic. This LED blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet link not working or the port is shutdown. On autonomous access points, this LED also provides signal strength readings during installation mode.

When the lightweight access point is searching for a controller, the Radio, Status, and Ethernet LEDs sequentially blink green, red and amber.

For additional information on the LEDs, refer to the "Checking the LEDs on an Autonomous Access Point/Bridge" section on page 4-2 or the "Checking the LEDs on Lightweight Access Points" section on page 5-2.

Operating Roles for the Autonomous Access Point/Bridge

The autonomous access point/bridge unit can be configured into one of seven operating roles from the Express Setup page:

Note The lightweight access point only supports the access point operating role.

- **Install Automatic**—Activates the bridge install and alignment mode. Specifies that the unit automatically determines the network role. If the unit is able to associate to another Cisco Aironet root bridge within 60 seconds, the unit assumes a non-root bridge role. If the unit is unable to associate with another Cisco Aironet root bridge within 60 seconds, the unit assumes a root bridge role.

  You can also pre-configure the unit into root bridge or non-root bridge modes and avoid the 60-second automatic detection phase.
- **Install Root Bridge**—Activates the root bridge install and alignment mode. Specifies that the unit is configured as a root bridge and accepts associations with non-root bridges.
- **Install Non-Root Bridge**—Activates the non-root bridge install and alignment mode. Specifies that the unit is configured as a non-root bridge and attempts to associate with a root bridge.
- **Root Bridge**—Specifies that the unit is operating as a root bridge and that it connects directly to the main Ethernet LAN network. In this mode, the unit accepts associations from other Cisco Aironet bridges and wireless client devices.
- **Non-Root Bridge**—Specifies that the unit is operating as a non-root bridge, that it connects to a remote LAN network, and that it must associate with a Cisco Aironet root bridge using the wireless interface.
- **Root Bridge with Wireless Clients**—Specifies that the unit is operating as a root bridge and accepts wireless client associations.
- **Non-Root Bridge with Wireless Clients**—Specifies that the unit is operating as a non-root bridge and accepts wireless client associations.
- **Access Point**—Specifies that the unit operates as an access point connected to the main Ethernet LAN network. In this mode, wireless client devices are allowed to associate to the unit.
- **Repeater**—Specifies that the unit is operating as a repeater (also called *repeater non-root*) that is not connected to the wired LAN and supports wireless clients.
- **Workgroup Bridge**—Specifies that the unit operates as a workgroup bridge connected to a small wired Ethernet LAN network through an Ethernet hub or switch. The workgroup bridge must associate to a Cisco Aironet access point or a Cisco Aironet bridge.
- **Scanner**—This setting is enabled when your product is being used by the Cisco WLSE to monitor wireless data traffic.

Note On initial power up, an autonomous access point/bridge running Cisco IOS Release 12.3(2)JA2 and earlier defaults to the Install-Mode role. On initial power up, an autonomous access point/bridge running Cisco IOS Release 12.3(4)JA or later defaults to the Root AP role.

Refer to the *Cisco IOS Software Configuration Guide for Access Points* and to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for additional information on the operating modes supported by the unit.

Network Examples with Autonomous Access Point/Bridges

This section describes the autonomous access point/bridge's role in three common wireless network configurations. The unit's default configuration is an access point.

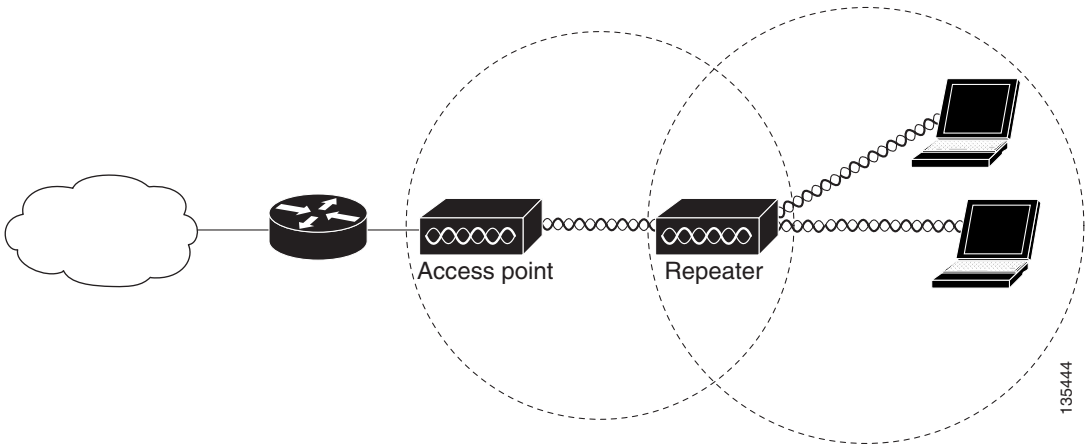
The autonomous 1300 series access point/bridge can be configured in access point, repeater, bridge, and workgroup bridge wireless operating modes.

Repeater Unit that Extends Wireless Range

An autonomous access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-4 shows an autonomous access point acting as a repeater. Consult the *Cisco IOS Software Configuration Guide for Access Points* for instructions on setting up an access point as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

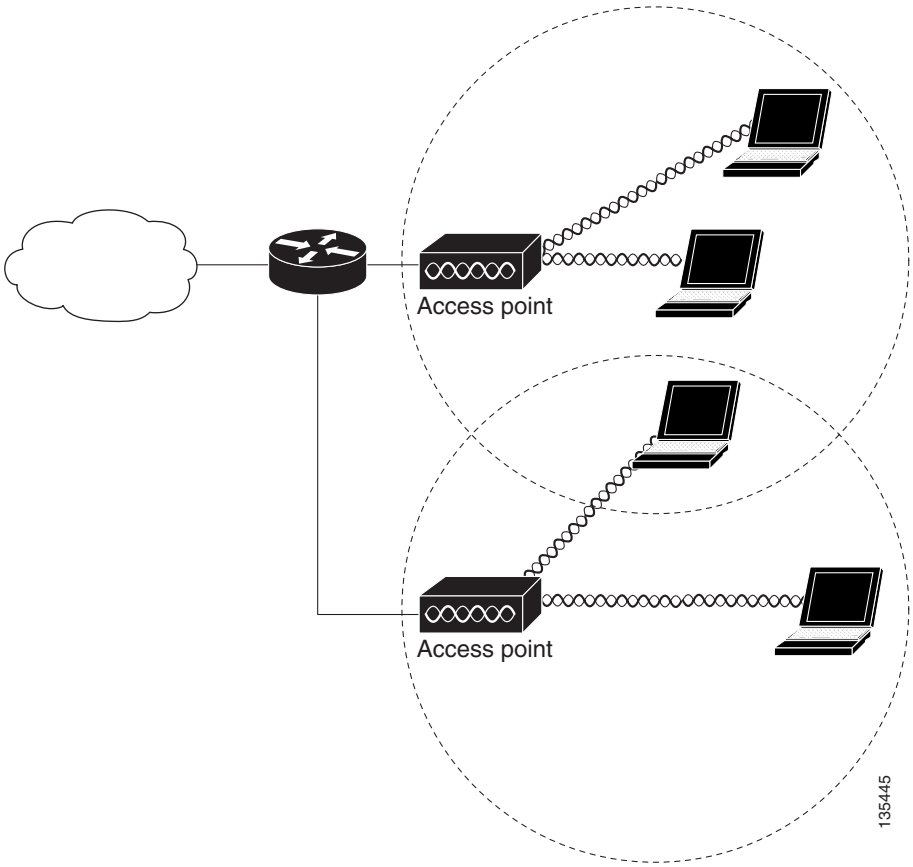
Figure 1-4 Access Point as Repeater



Root Access Point on a Wired LAN

An autonomous access point connected directly to a wired LAN provides a connection point for wireless users. If more than one autonomous access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-5 shows access points acting as root units on a wired LAN.

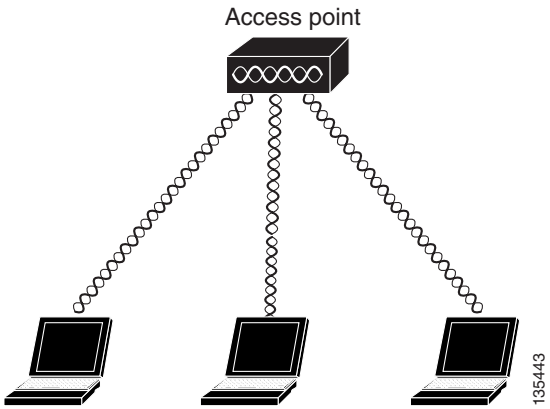
Figure 1-5 Access Points as Root Units on a Wired LAN



Central Unit in an All-Wireless Network

In an all-wireless network, an autonomous access point acts as a stand-alone root unit. The autonomous access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-6 shows an autonomous access point in an all-wireless network.

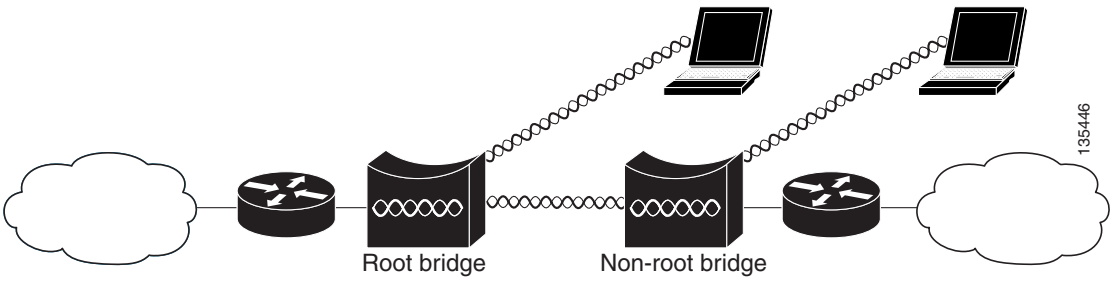
Figure 1-6 Access Point as Central Unit in All-Wireless Network



Bridge Network with Wireless Clients

The access point supports root bridge and non-root bridge roles used to interconnect a remote LAN to the main LAN (see Figure 1-7). The bridge units can also support wireless clients.

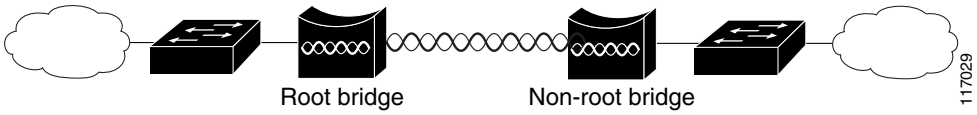
Figure 1-7 Root Bridge and Non-Root Bridge with Clients



Point-to-Point Bridge Configuration

In a point-to-point bridge configuration, two bridges interconnect two LAN networks using a wireless communication link (see Figure 1-8). The bridge connected to the main LAN network is classified as a root bridge and the other bridge is classified as a non-root bridge.

Figure 1-8 Point-to-Point Bridge Configuration



Workgroup Bridge Network

The access point supports a workgroup bridge role to interconnect remote Ethernet workstations to the main LAN. The workgroup bridge can communicate with an access point (see Figure 1-9) or with a bridge (see Figure 1-10).

Figure 1-9 Workgroup Bridge Communicating with an Access Point

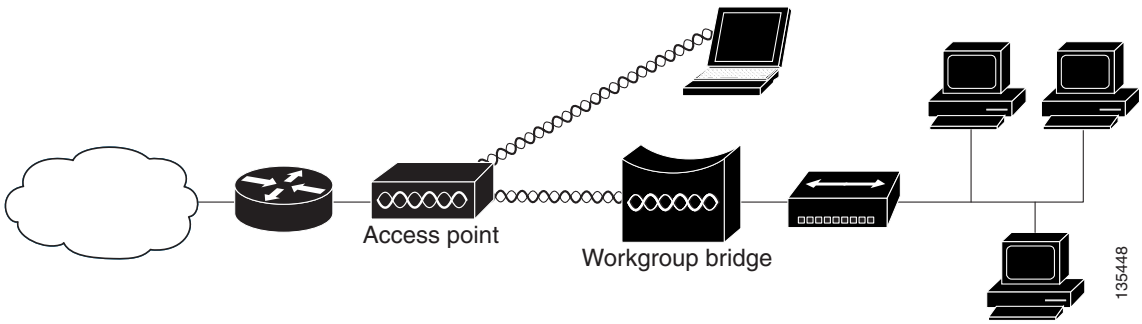
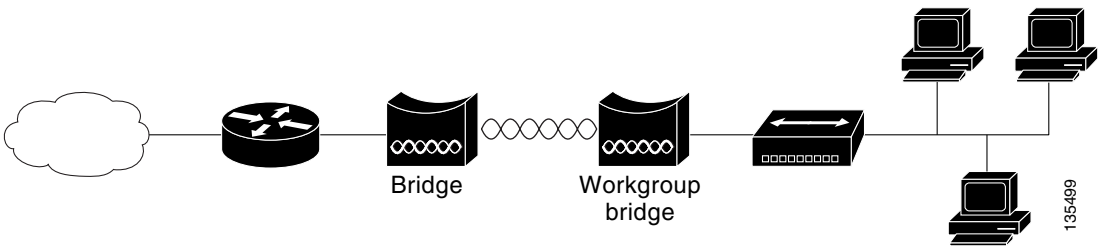


Figure 1-10 Workgroup Bridge Communicating with a Bridge

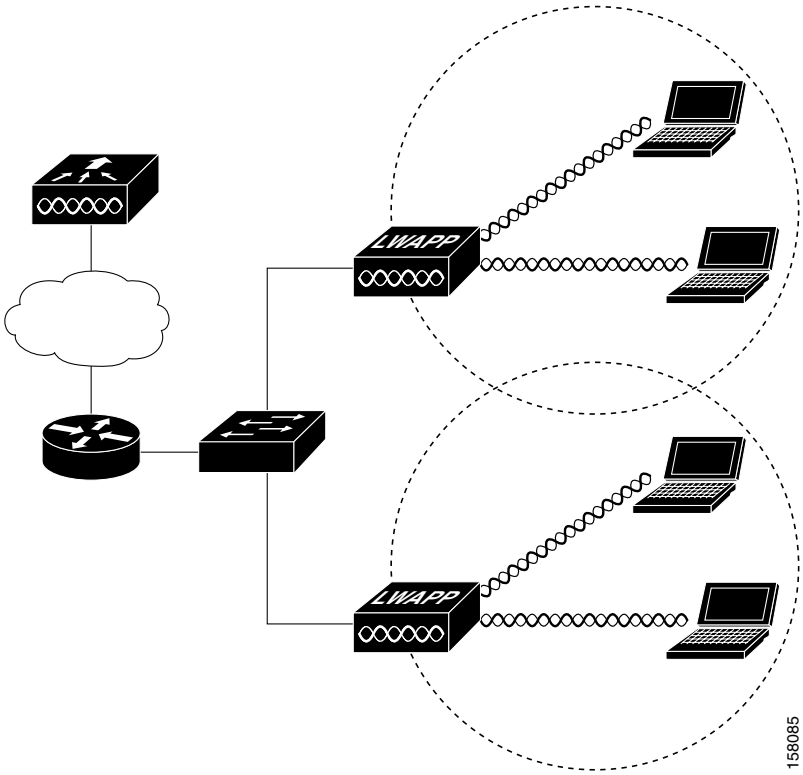


Network Examples with Lightweight Access Points

The lightweight access points support Layer 3 network operation. Lightweight access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

This section illustrates a typical wireless network configuration containing lightweight access points and a Cisco Wireless LAN Controller (see Figure 1-11).

Figure 1-11 Typical Lightweight Access Point Network Configuration Example



CHAPTER 2

Installation Overview

This chapter provides warnings, safety information, and information needed before you begin the installation of your access point/bridge system. This chapter includes the following sections:

Safety Warnings

Translated versions of all safety warnings are available in the safety warning document that shipped with your access point or on Cisco.com. To browse to the document on Cisco.com, refer to Appendix A, "Translated Safety Warnings" for instructions.

All Installations

Warning **IMPORTANT SAFETY INSTRUCTIONS**
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071
SAVE THESE INSTRUCTIONS

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **In order to comply with international radio frequency (RF) exposure limits, dish antennas should be placed at a minimum of 8.7 inches (22 cm) from the bodies of all persons. Other antennas should be placed a minimum of 7.9 inches (20 cm) from the bodies of all persons.** Statement 346

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A** Statement 1005

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper**

installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).
Statement 1052

Outdoor and DC Power Source Installations

The following warning applies to outdoor and DC power source installations:

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

DC Power Source Installations

The following warnings apply to DC power source installations using the optional LR2T power injector:

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.** Statement 1022

Warning **Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards.** Statement 1033

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the access point/bridge.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**
Statement 1052

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, please read and follow these safety precautions. They may save your life!

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance.
2. Select your installation site with safety, as well as performance in mind. Remember: electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successful raising of a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task, and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing your antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember, the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line complete an electrical path through the antenna and the installer: you!
7. If any part of the antenna system should come in contact with a power line, don't touch it or try to remove it yourself. Call your local power company. They will remove it safely.

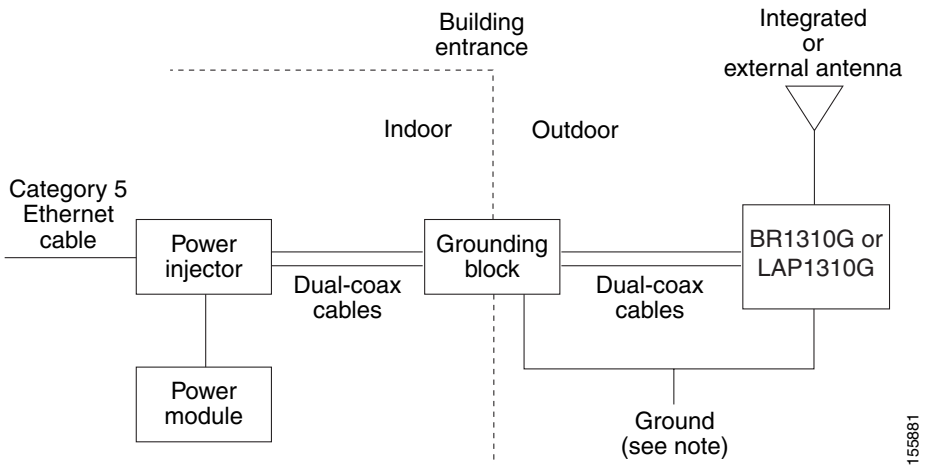
If an accident should occur with the power lines call for qualified emergency help immediately.

Typical Outdoor Installation Components

The access point/bridge is designed to be installed in an outdoor environment, typically on a tower or a tall building. A typical outdoor installation diagram is shown in Figure 2-1.

Note The lightweight access point can only operate as an access point.

Figure 2-1 Typical Outdoor Installation Diagram



Note Ground wires must comply with Sections 810 and 820 of the National Electrical Code and Section 54 of the Canadian Electrical Code.

Caution To ensure correct installation and grounding, install the access point/bridge in compliance with your local and national electrical codes: National Fire Protection Association (NFPA) 70, National Electrical Code (U.S.); Canadian Electrical Code, Part I, CSA 22.1 (Canada); and if local or national electrical codes are not available, refer to IEC 364, Part 1 through 7 (other countries).

Note The grounding block is not required for indoor installations of the access point/bridge and antenna.

Installation Guidelines

Because the access point/bridge is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- Install the access point/bridge in an area where structures, trees, or hills do not obstruct radio signals to and from the unit.
- Install the access point/bridge at a height sufficient to provide a clear line-of-sight signal path.

Site Surveys

Every network application is a unique installation. Before installing multiple access point/bridges, you should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary because the extra height also increases potential interference from other unlicensed radio systems.
- Physical environment—Clear or open areas provide better radio range than closed or filled areas.
- Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.

Unpacking the Access Point/Bridge

Follow these steps to unpack the access point/bridge:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the "Package Contents" section are included in the shipment. If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each access point/bridge package contains these items:

- An access point/bridge unit (model: AIR-BR1310G or AIR-LAP1310G)
  - Integrated antenna or external antenna configuration
- Power injector (LR2) unit
- Power module and AC power cord
- Quick start guide
- Mounting instructions document
- Read Me document
- Translated safety warnings document
- Cisco product registration and Cisco documentation feedback cards

Note The external antenna access point/bridge configuration does not ship with an external antenna. An external antenna must be purchased.

The optional roof mount kit contains these items:

- One roof-wall mount
- Two dual-coax cables [20 ft (6.1 m) and 50 ft (15.2 m)]
- Multi-function mount (consisting of a access point/bridge bracket and a mast bracket)
- Two tower clamps (U-bolts) with four nuts and washers
- Four bolts and washers for securing the access point/bridge bracket to the mast bracket
- Four bolts for securing the access point/bridge bracket to the unit
- Grounding block and mounting screws
- Ground lug for the access point/bridge, two hex nuts, and two washers
- Weatherproofing kit (consisting of Coax Seal and electrical joint compound)

The optional wall mount kit (for indoor use) contains these items:

- Wall mount bracket with 4 mounting bolts and washers
- Two sub-mini RG-59 coax cables (12 in. or 30.5 cm)

The optional transportation power injector

- Power injector (LR2T) unit

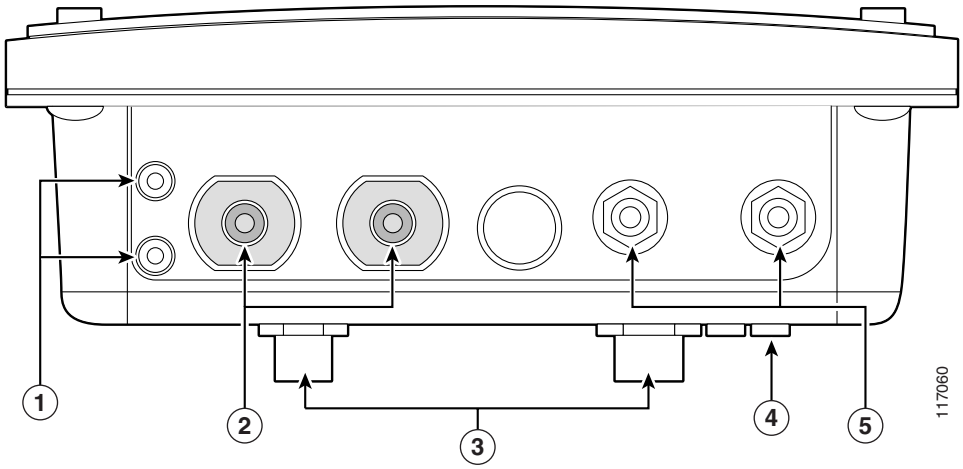
Before Beginning the Installation

Before you begin the installation process, please carefully review the following list of figures to become familiar with the system components, connectors, indicators, cables, system interconnection, and grounding:

- Installation diagram (Figure 2-1)
- Access point/bridge layout (Figure 2-2)
- Power injector layout (Figure 2-3)
- Power module (Figure 2-4)
- Grounding block (Figure 2-5)

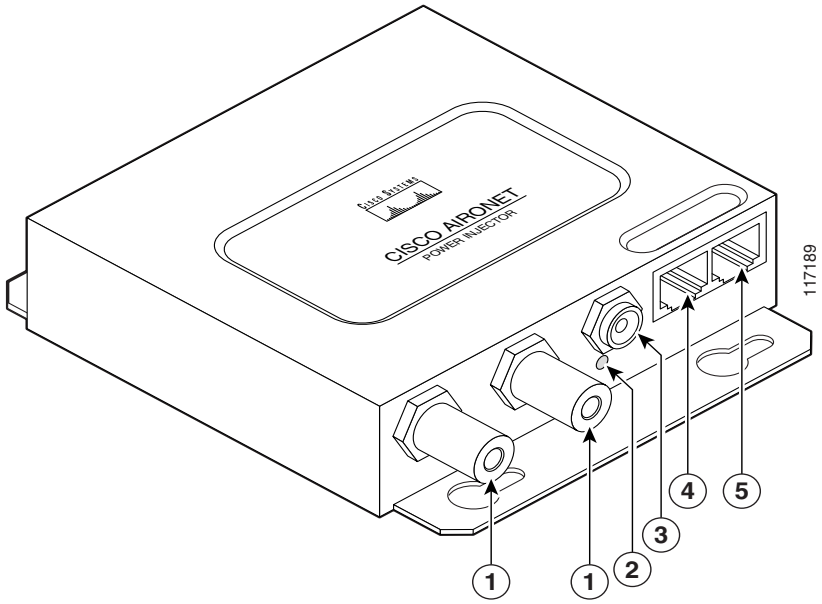
Note To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password-protected by the network administrator to maintain regulatory compliance.

Figure 2-2 Access Point/Bridge Layout



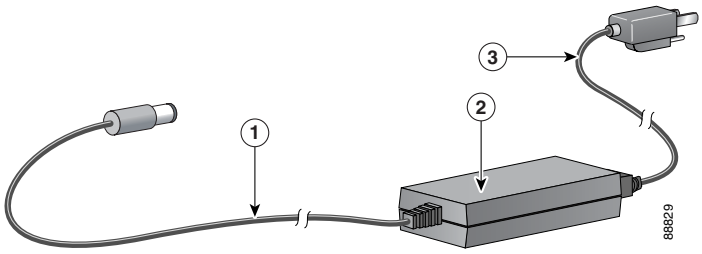
1	Grounding studs	**4**	LEDs
2	Antenna connectors	**5**	Dual-coax Ethernet ports (F-Type connectors)
3	Mounting lugs		

Figure 2-3 Power Injector Indicators and Connectors



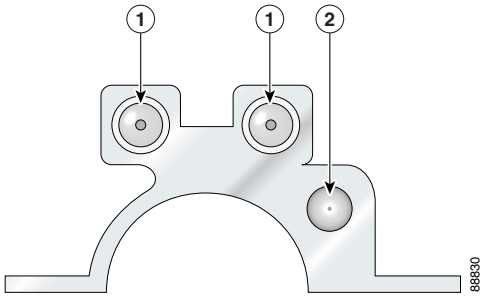
1	Dual-coax Ethernet ports (F-Type connectors)	**4**	Ethernet LAN port (RJ-45 connector)
2	Power LED	**5**	Console serial port (RJ-45 connector)
3	Power jack		

Figure 2-4 Power Module



1	48-VDC power output cable	**3**	AC power cord
2	Power module		

Figure 2-5 Grounding Block



1	F-type coaxial connectors	**2**	Ground wire lug

Installation Summary

Caution You should read and carefully follow the installation instructions before connecting the system to its power source. The access point/bridge and power injector can be damaged by incorrect power application.

Note To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administrator or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password-protected by the network administrator to maintain regulatory compliance.

During the installation of the access point/bridge, you will perform the following operations:

- Connect a user-supplied Category 5 Ethernet cable from your wired LAN network to the power injector.

- For outdoor installations, connect the dual-coax Ethernet cables between the power injector and the grounding block. For indoor installations, connect the dual-coax cables to the power injector.

Tip You can connect the dual-coax cable connectors to either of the grounding block connectors or the power injector's dual-coax Ethernet ports. The access point/bridge senses the Ethernet signals and automatically switches internal circuitry to match the cable connections.

Note You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

- For outdoor installations, connect a ground wire to the grounding block.
- Mount the access point/bridge to the mast, tower, or wall. For additional information, refer to the mounting instructions that shipped with your access point/bridge.

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

- Connect a ground wire to the access point/bridge (use the ground lug).
- For outdoor installations, connect the dual-coax Ethernet cables to the grounding block and to the access point/bridge. For indoor installations, connect the dual-coax cables directly to the access point/bridge.

Tip You can connect the dual-coax cable connectors to either of the grounding block connectors or the access point/bridge's dual-coax ports. The access point/bridge senses the Ethernet signals and automatically switches internal circuitry to match the cable connections.

Note You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A** Statement 1005

- For indoor installations, connect these items:
  - The AC power cord to the 48-VDC power module.
  - The power module power plug to the power injector and plug the AC cord into an AC power receptacle.
- For outdoor installations, refer to the mounting instruction document that shipped with your access point/bridge.
- Seal all external connectors with special weather sealing material.

Configure security and other access point/bridge options. For additional information, refer to the *Cisco IOS Software Configuration Guide for Access Points* or the *Cisco Wireless LAN Controller Configuration Guide*.

CHAPTER 3

Mounting Overview

This chapter provides an access point/bridge mounting overview. The following sections are included in this chapter:

Mounting the Access Point/Bridge

Typically, the access point/bridge is installed on a rooftop, mast, tower, wall, or a suitable flat surface. Each of these installations requires a different approach. This document provides a mounting overview. For detailed mounting instructions, refer to the mounting instructions that shipped with your unit.

The access point/bridge is available in two configurations:

- Integrated antenna access point/bridge (with 13-dBi)
- External antenna access point/bridge (with two antenna connectors for use with a single antenna or dual diversity antennas)

Note Personnel installing the access point/bridge must understand wireless techniques, antenna mounting and adjustment, and grounding methods.

Note To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password-protected by the network administrator to maintain regulatory compliance.

The following warning applies to outdoor and vehicle installations:

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Mounting Hardware

The access point/bridge supports the following optional mounting kits:

- The roof mount kit (for indoor or outdoor use) contains these items:
  - One roof-wall mount
  - Two dual-coax cables [20 ft (6.1 m) and 50 ft (15.2 m)]
  - Multi-function mount (consisting of a access point/bridge bracket and a mast bracket)
  - Two tower clamps (U-bolts) with four nuts and washers
  - Four bolts and washers for securing the access point/bridge bracket to the mast bracket
  - Four bolts for securing the access point/bridge bracket to the unit
  - Grounding block and mounting screws
  - Ground lug for the access point/bridge, two hex nuts, and two washers
  - Weatherproofing kit (consisting of Coax Seal and electrical joint compound)
- The wall mount kit (for indoor use) contains these items:
  - Wall mount bracket with 4 mounting bolts and washers
  - Two sub-mini RG-59 cables (12 in or 30.5 cm)

Window Mounting

When a wireless link is deployed through a window, significant signal loss can be introduced by the window. Typical losses range from 5 to15 dB per window, depending upon the type of glass. You should take this extra loss into account when planning antenna gains and power settings. A thorough site survey is critical for deployments through windows.

For additional information on a window mounting bracket, refer to the following URL:

http://www.terrawave.com/BR1300

Multi-Function Mount

The multi-function mount provides a method for mounting the access point/bridge on a mast, tower, or a roof mount and consists of two parts (see Figure 3-1):

- An access point/bridge bracket—attaches to the back of the unit
- A mast bracket—attaches to the mast, tower, or roof mount

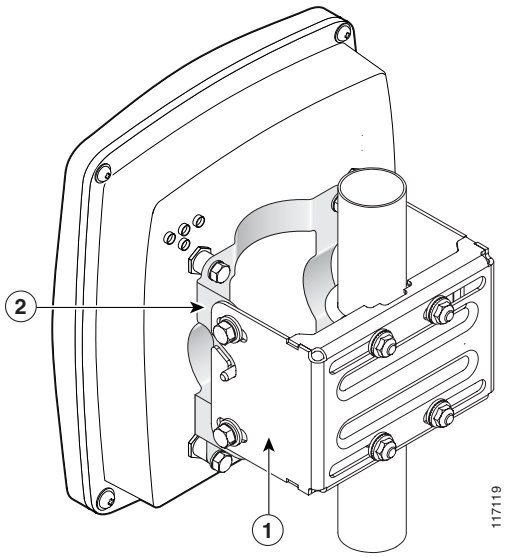
The multi-function mount permits easy azimuth and elevation adjustments. The basic mounting procedure is shown below:

1. Mount the access point/bridge bracket to the mounting lugs on the access point/bridge.
2. Mount the mast bracket to the tower or mast using the supplied U-bolts or appropriately sized user-supplied U-bolts.
3. Suspend the access point/bridge on the mast bracket using the support pins.
4. Secure the access point/bridge bracket to the mast bracket using the supplied nuts, bolts, and washers (hand tighten).
5. Connect the dual-coax cable to the power injector dual-coax Ethernet ports (F-type connectors) on the access point/bridge.

Note You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

6. Connect the ground wire to the outdoor mounted access point/bridge using the supplied ground lug.
7. Connect the power cable to the power injector.
8. Tighten the nuts and bolts.

Figure 3-1 Multi-Function Mount



1	Access point bracket with support pins	**2**	Mast bracket

Access Point Bracket

The access point/bridge bracket mounts on the back side of the unit housing. The bracket mounts on four lugs on the unit. The bracket contains two support pins that are used to suspend the unit in the notches on the mast mounting bracket until you secure the mounting bolts.

The access point/bridge must be positioned to obtain the correct antenna polarization that matches the remote antenna. The integrated access point/bridge antenna is vertically polarized. All access point/bridges must use the same antenna polarization for best operation.

Mast Bracket

The mast bracket attaches to a mast or tower support and is used to secure the access point/bridge (see Table 3-1).

Table 3-1 Mast Bracket Attachment Methods

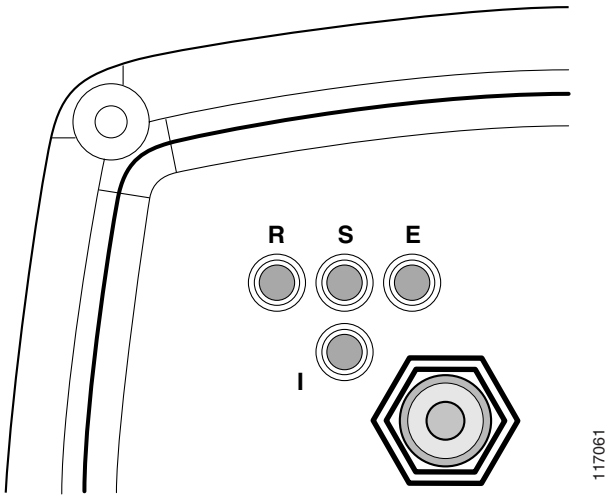
Mast Type	Mast Diameter	Mast Attachment Method
Roof mount, small mast, or tower	1.5 to 2.75 in. (30.5 to 69.9 mm)	Attach the pipe inside the mounting bracket, between the bracket and access point/bridge.

Note The U-bolts provided with the roof mounting kit support mast diameters up to 1.75 in. (44.5 mm). For larger masts, you must supply the U-bolts to attach the access point/bridge.

LEDs

The LEDs indicate the status, radio activity, and Ethernet activity. The LEDs are mounted on the back of the housing (see Figure 3-2).

Figure 3-2 LEDs



R	Radio LED	**E**	Ethernet LED
S	Status LED	**I**	Install LED

For additional information on LED indications, refer to the "Troubleshooting Autonomous Access Points and Bridges" section on page 4-1 or the "Troubleshooting Lightweight Access Points" section on page 5-1.

Autonomous Access Point/Bridge

When the autonomous access point/bridge running Cisco IOS Release 12.3(4)JA is initially powered-up, the unit defaults to a root access point with the radio disabled and no default SSID. To allow client associations, you must configure an SSID and enable the radio interface (refer to the *Cisco IOS Software Configuration Guide for Access Points*).

When the autonomous access point/bridge running Cisco IOS Release 12.3(2)JA2 and earlier is initially powered-up, the bridge installation mode is activated and the unit attempts to associate to a root bridge for 60 seconds. If it is unable to associate with a root bridge, it automatically assumes the root bridge role.

The Install LED provides bridge association status during installation mode as shown in Table 3-2.

Table 3-2 Install LED Status

Install LED	Status	Bridge State
Off	Self test	Startup.
Amber blinking	Non-root, searching	Not associated (non-root mode). The access point/bridge attempts to associate with a root bridge for 60 seconds[1].
Amber	Non-root, associated	Associated (non-root mode).
Green blinking	Root, searching	Not associated (root mode). The access point/bridge attempts to associate with a non-root bridge indefinitely.
Green	Root, associated	Associated (root mode).
Red	Error	Overvoltage or overcurrent error[2]

1. Preconfigured bridges search indefinitely.
2. Disconnect power to the power injector, wait approximately 1 minute, and reconnect power. If error continues, contact technical support.

Use the Install LED to determine when the bridge successfully associates with a remote bridge and to verify its mode of operation. After association, the other three LEDs indicate signal strength.

The startup and association sequence depends on the access point/bridge configuration, which can be one of the following types:

- Default—The access point/bridge attempts to associate with a root bridge for 60 seconds. If it does not associate with a root bridge, it attempts to associate with a non-root bridge.
- Preconfigured bridge mode—The unit attempts to associate with a remote bridge in the configured mode, either root or non-root. Because there are no timeouts, it is easier to align the antenna.
- Preconfigured access point or workgroup bridge modes—the bridge Install LED does not operate.

Aligning the Autonomous Bridge Antenna Using RSSI LED Indications

For the autonomous bridge, you can align the integrated antenna using LEDs after the unit successfully associates with a remote bridge. In the installation mode before association to another bridge, the Install LED blinks amber. If the unit associates to a root bridge, the Install LED turns amber. If the unit does not associate to a root bridge in the first 60 seconds, the Install LED blinks green to indicate that beacons are being transmitted and that the unit is waiting for another non-root bridge to associate.

During the first 20 seconds after association, the unit reads the receive signal strength indictor (RSSI) levels and records the maximum level received. After 20 seconds have elapsed, the Install LED turns amber and the Ethernet, status, and radio LEDs display the relative RSSI levels compared to the maximum received. The RSSI LED indications are shown in Table 3-3).

Note For the signal level (dBm), a smaller number represents a stronger signal because the signal level is given as a negative value.

Table 3-3 Bridge LED Installation Mode RSSI Display

RSSI Level (dBm)	Ethernet LED	Status LED	Radio LED
> –44	On	On	On
–47 to –44	Fast blink[1]	On	On
–50 to –47	Medium blink[2]	On	On
–53 to –50	Slow blink[3]	On	On
–54 to –53	Off	On	On
–57 to –54	Off	Fast blink[1]	On
–60 to –57	Off	Medium blink[2]	On
–63 to –60	Off	Slow blink[3]	On
–66 to –63	Off	Off	On
–69 to –66	Off	Off	Fast blink[1]
–72 to –69	Off	Off	Medium blink[2]
–75 to –72	Off	Off	Slow blink[3]
< –75	Off	Off	Off

1. Slow blinking rate of 1 blink/sec.
2. Medium blinking rate of 2 blinks/sec.
3. Fast blinking rate of 4 blinks/sec.

When using LEDs to maximize the signal, adjust the antenna until as many LEDs as possible are turned on and the rest are blinking as fast as possible.

Troubleshooting Autonomous Access Points and Bridges

This chapter provides troubleshooting procedures for basic problems with the autonomous access point/bridge (model: AIR-BR1310G). For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

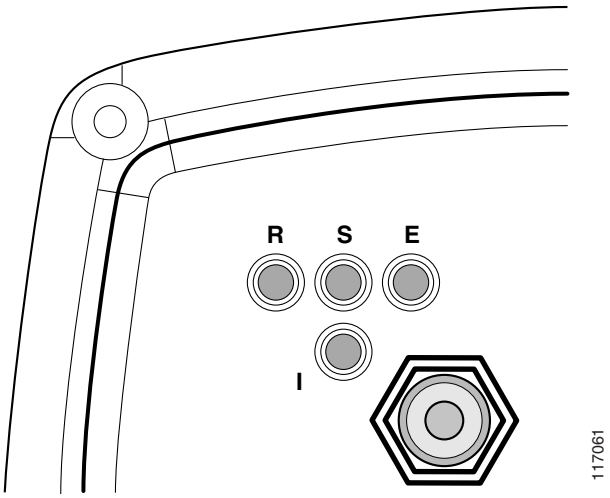
Sections in this chapter include:

Checking the LEDs on an Autonomous Access Point/Bridge

If your autonomous access point/bridge is not associating with a remote bridge or a wireless client, check the four LEDs on the back panel. You can use them to quickly assess the unit's status. For information on using the LEDs during the installation and alignment of the antenna, refer to the "LEDs" section on page 3-5.

Figure 4-1 shows the access point/bridge LEDs.

Figure 4-1 LEDs



R	Radio LED	**E**	Ethernet LED
S	Status LED	**I**	Install LED

Normal Mode LED Indications for an Autonomous Access Point/Bridge

During normal operation of your autonomous access point/bridge the LEDs provide status information as shown in Table 4-1.

Table 4-1 LED Indications

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
Off	—	—	—	Ethernet link is down or disabled.
Blinking green	—	—	—	Transmitting and receiving Ethernet packets.
Blinking amber	—	—	—	Transmitting and receiving Ethernet errors.
amber	—	—	—	Firmware error—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.

Table 4-1 LED Indications (continued)

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
—	Blinking green	—	—	Root bridge mode—no remote bridges are associated. Non-root bridge mode—not associated to the root bridge. If all bridges are powered up, this could be caused by incorrect SSID and security settings or improper antenna alignment. You should check the SSID and security settings of all bridges and verify antenna alignment. If the problem continues, contact technical support for assistance.
—	Green	—	—	Root mode—associated to at least one remote bridge. Non-root mode—associated to the root bridge. This is normal operation.
—	Blinking amber	—	—	General warning—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Amber	—	—	Loading firmware.
Red	Amber	Red	—	Loading Firmware error—disconnect and reconnect the power injector power. If the problem continues, contact technical support for assistance.
—	—	Off	—	Normal operation.
—	—	Blinking green	—	Transmitting and receiving radio packets—normal operation.
—	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio interface—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	—	Amber	—	Radio firmware error—disconnect and reconnect power injector power. If the problem continues, contact technical support for assistance.
—	—	—	Amber blinking	Not associated (non-root mode). The access point/bridge attempts to associate with a root bridge for 60 seconds[1].
—	—	—	Amber	Associated (non-root mode).
—	—	—	Green blinking	Not associated (root mode). The access point/bridge attempts to associate with a non-root bridge indefinitely.
—	—	—	Green	Associated (root mode).
—	—	—	Red	Overcurrent or overvoltage error—disconnect power to the power injector, check all coax cable connections, wait approximately 1 minute, and reconnect power. If error continues, contact technical support.

1. Preconfigured bridges search indefinitely.

The autonomous access point/bridge uses a blinking code to identify various error conditions. The code sequence uses a two-digit diagnostic code that starts with a long pause to delimit the code, followed by the LED flashing red to count out the first digit, then a short pause, followed by the LED flashing red to count out the second digit.

The LED blinking error codes are described in Table 4-2.

Table 4-2 LED Blinking Error Codes on an Autonomous Access Point/Bridge

LED	Blinking Codes		Description
	First Digit	Second Digit	
Ethernet	2	1	Ethernet cable problem—verify that the cable is properly connected and not defective. This error might also indicate a problem with the Ethernet link. If the cable is connected properly and not defective, contact technical support for assistance.
Radio	1	2	Radio not detected—contact technical support for assistance.
	1	3	Radio not ready—contact technical support for assistance.
	1	4	Radio did not start—contact technical support for assistance.
	1	5	Radio failure—contact technical support for assistance.
	1	6	Radio did not flash its firmware—contact technical support for assistance.

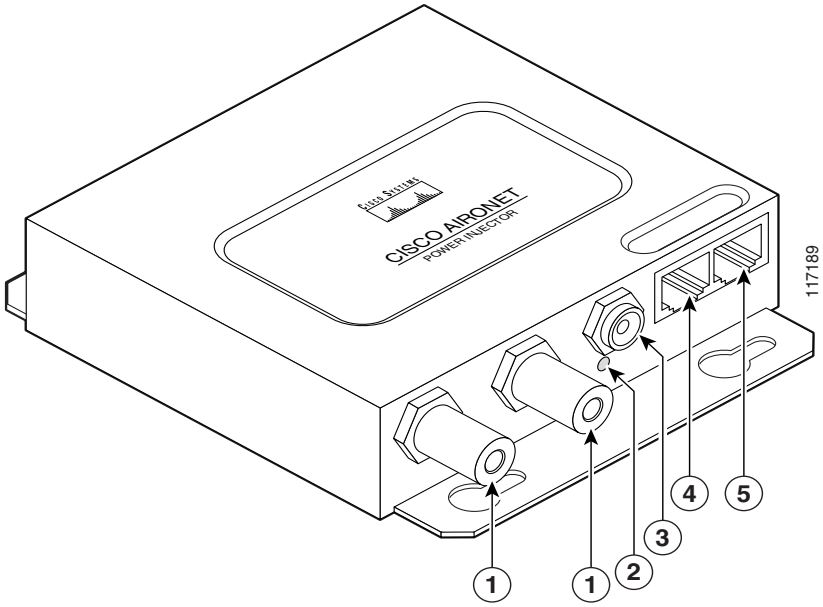
Power Injector

When the power injector is powered up, it applies 48-VDC to the dual-coax cables to the access point/bridge.

When power is applied to the access point/bridge, the unit activates the bootloader and begins the POST operations. The access point/bridge begins to load the Cisco IOS image when the POST operations are successfully completed. Upon successfully loading the image, the unit initializes and tests the radio.

The power injector LED is shown in Figure 4-2.

Figure 4-2 Power Injector



1	Dual-coax Ethernet ports (F-Type connectors)	**4**	Ethernet LAN port (RJ-45 connector)
2	Power LED	**5**	Console serial port (RJ-45 connector)
3	Power jack		

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the bridge)
  - 48-VDC input power
  - Uses the 48-VDC power module (included with the bridge)
- Cisco Aironet Power Injector LR2T—optional transportation version
  - 12- to 40-VDC input power
  - Uses 12 to 40 VDC from a vehicle battery

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector LED (see Figure 4-2):

- Power LED
  - Green color indicates input power is being supplied to the bridge.
  - Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.

Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

  - Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Checking Basic Configuration Settings

Mismatched basic settings are the most common causes of lost wireless connectivity. Check the following areas.

Default IP Address Behavior

When you connect an autonomous access point/bridge running Cisco IOS Release 12.3(2)JA or later software with a default configuration to your LAN, the access point/bridge requests an IP address from your DHCP server and, if it does not receive an IP address, continues to send requests indefinitely. To eliminate this behavior, you must access the access point/bridge through its console port and assign a static IP address.

When you connect an autonomous access point/bridge running Cisco IOS Release 12.2(15)JA2 or earlier software with a default configuration to your LAN, the access point/bridge requests an IP address from your DHCP server and, if it does not receive an IP address, it assigns a default IP address of 10.0.0.1

Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA2 and earlier, on initial power up the access point/bridge defaults to the Install-Mode role with the radio enabled and supports these SSIDs:

- SSID is *autoinstall* for the Install-Mode role.
- SSID is *tsunami* for Root AP and Workgroup Bridge roles.

In Cisco IOS Release 12.3(4)JA or later, on initial power up the access point/bridge defaults to the Root AP role with the radio disabled and no default SSID configured.

Note In Cisco IOS Release 12.3(4)JA or later, you must create an SSID and enable the radio before the access point/bridge allows wireless associations from other devices. These changes to the default configuration improve the security of a newly installed access point/bridge. Refer to the *Cisco IOS Software Configuration Guide for Access Points* for instructions on configuring the SSID and to the "Enabling the Radio Interface" section on page 4-7 for instructions on enabling the radio interface.

Enabling the Radio Interface

To enable the radio interface, follow these instructions:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 When the Summary Status page displays, click **Network Interfaces > Radio0-802.11g** and the radio status page displays.

Step 4 Click **Settings** and the radio settings page displays.

Step 5 Click **Enable** in the Enable Radio field.

Step 6 Click **Apply**.

Step 7 Close your web-browser.

SSID

To associate, all bridges, access points, workgroup bridges, or client devices must use the same SSID. The bridge installation mode SSID is *autoinstall* and the normal mode default SSID is *tsunami*. You should verify that the SSID value shown on the Express Setup page is the same for all bridges, access points, workgroup bridges, or client devices. You should also verify that the bridges or access points are configured for the proper network role; only one bridge can be configured as the root bridge and only one access point can be configured as a root access point.

Note Access points and bridges are not designed to associate with each other. However, a workgroup bridge can associate to either a Cisco Aironet access point or a Cisco Aironet bridge.

Note In Cisco IOS Release 12.3(4)JA or later, there is no default SSID. You must configure an SSID and enable the radio interface to communicate with other wireless devices.

Security Settings

Remote Cisco Aironet bridges or client devices attempting to authenticate to your access point/bridge must support the same security options configured in the access point/bridge, such as WEP, EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a Cisco Aironet non-root bridge or a non-root access point is unable to authenticate to your root bridge or root access point, verify that the security settings are the same as your access point/bridge settings. For additional information, refer to the *Cisco IOS Software Configuration Guide for Access Points*.

Antenna Alignment

If your autonomous non-root bridges are unable to associate to your root bridge, you should verify the basic configuration settings on all bridges before attempting to verify antenna alignment (refer to *Cisco IOS Software Configuration Guide for Access Points*). If your basic configuration settings are correct, you can verify antenna alignment by using the Install mode RSSI LED indications. For additional information, refer to the "Aligning the Autonomous Bridge Antenna Using RSSI LED Indications" section on page 3-6.

For detailed alignment instructions, refer to the *Cisco Aironet 1300 Series Outdoor Bridge Mounting Instructions* that shipped with your access point/bridge.

Note To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password-protected by the network administrator to maintain regulatory compliance.

Running the Carrier Busy Test

You can use the carrier busy test to determine the least congested channel for the radio interface (802.11g). You should typically run the test several times to obtain the best results and to avoid temporary activity spikes.

Note The carrier busy test is primarily used for single access points or bridge environments. For sites with multiple access points, a site survey is typically performed to determine the best operating locations and operating frequencies for the access points.

Note All associated clients on the selected radio will be disassociated during the 6 to 8 seconds needed for the carrier busy test.

Follow these steps to activate the carrier busy test:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Network Interfaces** and the Network Interface Summary page appears.

Step 4 Choose the radio interface by clicking **Radio0-802.11G**. The radio status page appears.

Step 5 Click the **Carrier Busy Test** tab and the Carrier Busy Test page appears.

Step 6 Click **Start** to begin the carrier busy test.

When the test completes, the results are displayed on the bottom of the page. For each of the channel center frequencies, the test produces a value indicating the percentage of time that the channel is busy.

Running the Ping or Link Test

You can use the ping or link test to evaluate the communication link with an associated wireless device. The ping or link test provides two modes of operation:

- Uses a specified number of packets and then displays the test results.
- Continuously operates until you stop the test and then displays the test results.

Follow these steps to activate the ping or link test:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Association** and the main association page appears.

Step 4 Click the MAC address of an associated wireless device and the Statistics page for that device appears.

Step 5 Click the **Ping/Link Test** tab and the Ping/Link Test page appears.

Step 6 If you want to specify the number of packets to use in the test, follow these steps:

a. Enter the desired number of packets in the Number of Packets field.

b. Enter the desired packet size in the Packet Size field.

c. Click **Start**. The test automatically stops when all packets are used.

Step 7 If you want to use a continuous test, follow these steps:

a. Enter the desired packet size in the Packet Size field.

b. Click **Start** to activate the test.

c. When desired, click **Stop** to stop the test.

When the test stops, the test results are displayed at the bottom of the page. You should check for lost packets that might indicate a possible problem with the wireless link. For best results, you should perform this test several times.

Resetting the Autonomous Access Point/Bridge to the Default Configuration

You can use the web-browser interface or the CLI to reset the autonomous access point/bridge to a factory default configuration.

Note The following steps reset all configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

For additional information on access point/bridge default behavior, see the "Default IP Address Behavior" section on page 4-6 and the "Default SSID and Radio Behavior" section on page 4-6.

Using the Web-Browser Interface

Follow the steps below to delete the current configuration and return all autonomous access point/bridge settings to the factory defaults using the Web-browser interface.

Step 1 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 3 Click **System Software** and the System Software page appears.

Step 4 Click **System Configuration** and the System Configuration page appears.

Step 5 Click **Default**.

Note If the access point/bridge is configured with a static IP address, the IP address does not change.

Step 6 After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Access Points)*.

Using the CLI on an Autonomous Access Point/Bridge

From privileged EXEC mode, you can reset the autonomous access point/bridge configuration to factory default values using the CLI by following these steps:

Step 1 Enter **erase nvram:** to erase all NVRAM files including the startup configuration.

Step 2 Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*.

Step 3 Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.

Step 4 Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm]*.

Caution Interrupting the boot process will damage the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up*.

Step 5 After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Access Points*).

The access point/bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the unit's new IP address, you can use the **show interface bvi1** CLI command.

Reloading the Access Point/Bridge Image

If your access point/bridge has a firmware failure, you must reload the complete image file using the Web-browser interface or by using the console serial port. You can use the browser interface if the access point/bridge firmware is operational. However, you can use the console serial port when the access point/bridge has a corrupt image.

Web-Browser Interface

You can also use the Web-browser interface to reload the access point/bridge image file. The Web-browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your autonomous access point/bridge configuration is not changed when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point/bridge image file on your PC and download the image to the unit. Follow the instructions below to use the HTTP interface:

Step 1 The PC you intend to use must be configured with a static IP address in the same subnet as the access point.

Step 2 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**. An Enter Network Password window appears.

Step 3 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 4 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade page appears.

Step 5 Click **Browse** to locate the image file on your PC.

Step 6 Click **Upload**.

Step 7 After the access point/bridge reboots, you can reconfigure the unit by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Access Points*).

For additional information, click the **Help** icon on the Software Upgrade page.

Browser TFTP Interface

The TFTP interface enables you to use a TFTP server on a network device to load the access point/bridge image file. Follow the instructions below to use a TFTP server:

Step 1 The PC you intend to use must be configured with a static IP address in the same subnet as the access point.

Step 2 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**. An Enter Network Password window appears.

Step 3 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.The Summary Status page appears.

Step 4 Click **System Software** and then click **Software Upgrade**. The HTTP Upgrade page appears.

Step 5 Click **TFTP Upgrade**.

Step 6 Enter the IP address for the TFTP server in the TFTP Server field.

Step 7 Enter a filename for the access point/bridge image file (such as c1310-k9w7-tar.123-8.JA.tar) in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is in the TFTP root directory, enter only the filename.

Step 8 Click **Upload**.

Step 9 After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Access Points*).

For additional information click the **Help** icon on the Software Upgrade page.

Obtaining the Autonomous Access Point/Bridge Image File

The autonomous access point image file can be obtained from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/cisco/software/navigator.html

Note To download software from the Cisco.com software center, you must be a registered user. You can register from the web page.

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1300 Series** .

Step 3 Click **Cisco Aironet 1310 Access Point/Bridge**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1310-k9w7-tar.123-11.JA.tar.

Step 8 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 9 On the Security Information window, click **Yes** to display non-secure items.

Step 10 On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.

Step 11 If you checked No, enter the requested information and click **Submit**.

Step 12 Click **Yes** to continue.

Step 13 Click **DOWNLOAD**.

Step 14 Read and accept the terms and conditions of the Software Download Rules.

Step 15 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 16 Click **Save** to download your image file to your hard disk.

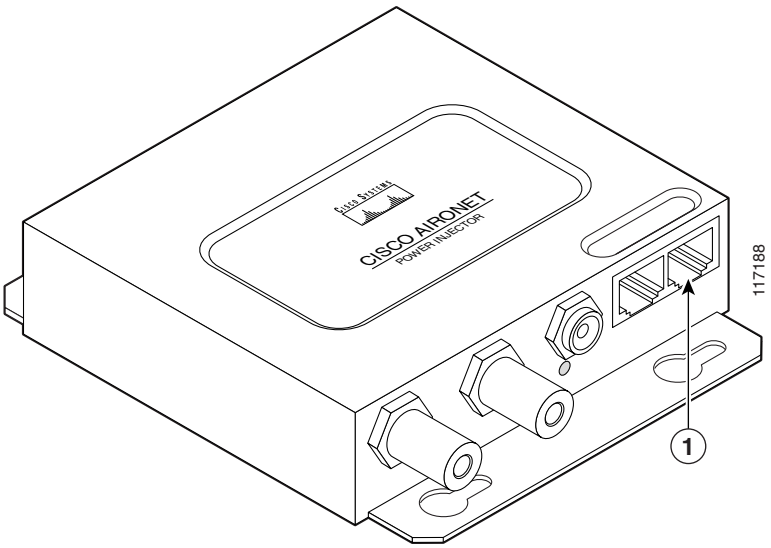
Step 17 Select the desired download location on your hard disk and click **Save**.

Connecting to the Console Serial Port

If you need to configure the access point locally (without connecting to a wired LAN), you can connect a PC to the power injector console serial port. Follow these steps to open the CLI by connecting to the console serial port:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial console port on the power injector and to the COM port on your PC. Figure 4-3 shows the power injector's console serial port connector.

Figure 4-3 Console Serial Port Connector



1	Console serial port connector (RJ-45 connector)	

Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3 When the terminal emulator is activated, press **Enter**.

Step 4 At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

Troubleshooting Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the lightweight access point (model: LAP1310G). For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

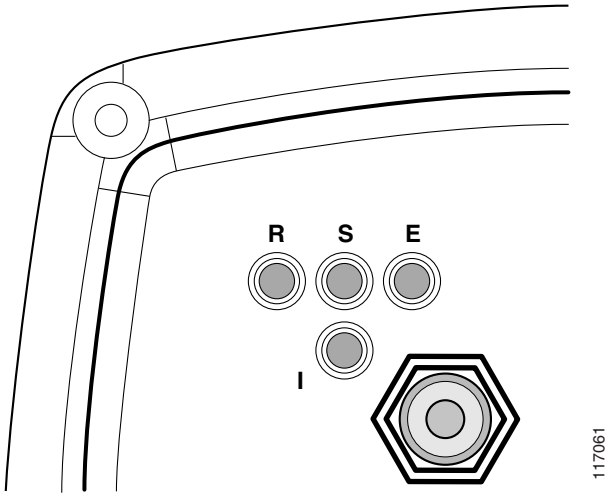
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

Checking the LEDs on Lightweight Access Points

If your lightweight access point is not operating properly, check the LEDs on the back panel. You can use them to quickly assess the unit's status. Figure 5-1 shows the access point LEDs.

Figure 5-1 LEDs



R	Radio LED	**E**	Ethernet LED
S	Status LED	**I**	Install LED

Note The Install LED is not used on the 1300 series lightweight access points.

LED Indications

During access point operation the LEDs provide status information as shown in Table 5-1.

Table 5-1 LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot loader errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	-	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware upgrade	–	Red	–	Loading new firmware image.

Table 5-1 LED Signals (continued)

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Controller status	Alternating green, red, and amber[1]			Connecting to the controller. **Note** If the access point remains in this mode for more than five minutes, the access point is unable to find the controller. Ensure a DHCP server is available or that controller information is configured on the access point.
Message type	**Ethernet LED**	**Status LED**	**Radio LED**	**Meaning**

1. This status indication has the highest priority and overrides other status indications.

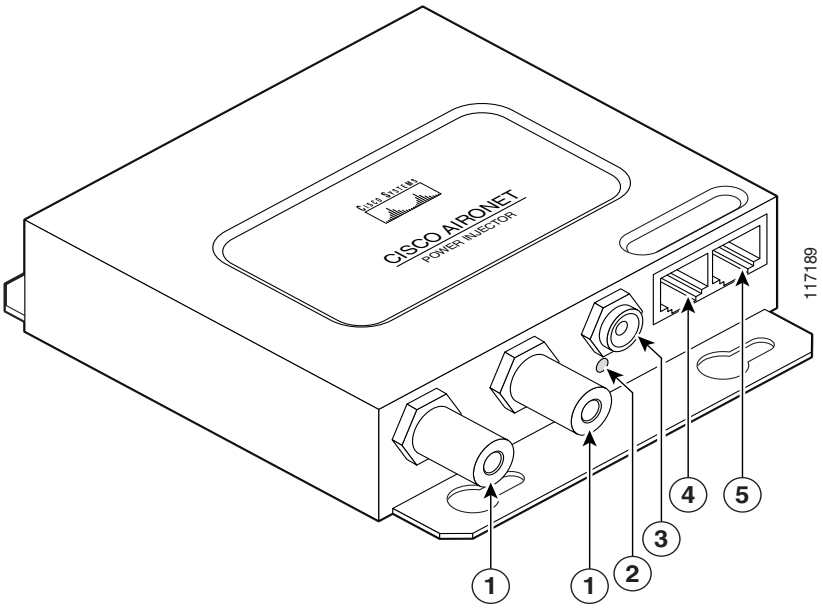
Power Injector

When the power injector is powered up, it applies 48-VDC to the dual-coax cables to the access point.

When power is applied to the access point, the unit activates the bootloader and begins the POST operations. The access point begins to load the Cisco IOS image when the POST operations are successfully completed. Upon successfully loading the image, the unit initializes and tests the radio.

The power injector LED is shown in Figure 5-2.

Figure 5-2 Power Injector



1	Dual-coax Ethernet ports (F-Type connectors)	**4**	Ethernet LAN port (RJ-45 connector)
2	Power LED	**5**	Console serial port (RJ-45 connector)
3	Power jack		

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the access point)
  - 48-VDC input power
  - Uses the 48-VDC power module (included with the access point)
- Cisco Aironet Power Injector LR2T—optional transportation version
  - 12- to 40-VDC input power

Checking Power

You can verify the availability of power to the lightweight access point by checking the power injector LED (see Figure 5-2):

- Power LED
  - Green color indicates input power is being supplied to the access point.
  - Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.

Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

  - Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the lightweight access points, enabling the access point to find and associate with a controller. For additional information, refer to the "Configuring DHCP Option 43 for Lightweight Access Points" section on page G-1.

Manually Configuring Controller Information Using the Access Point CLI

In a new installation, when your access point is unable to reach a DHCP server, you can manually configure needed controller information using the lightweight access point CLI.

Note The CLI commands in this section can be used only on a lightweight access point that is not associated to a controller.

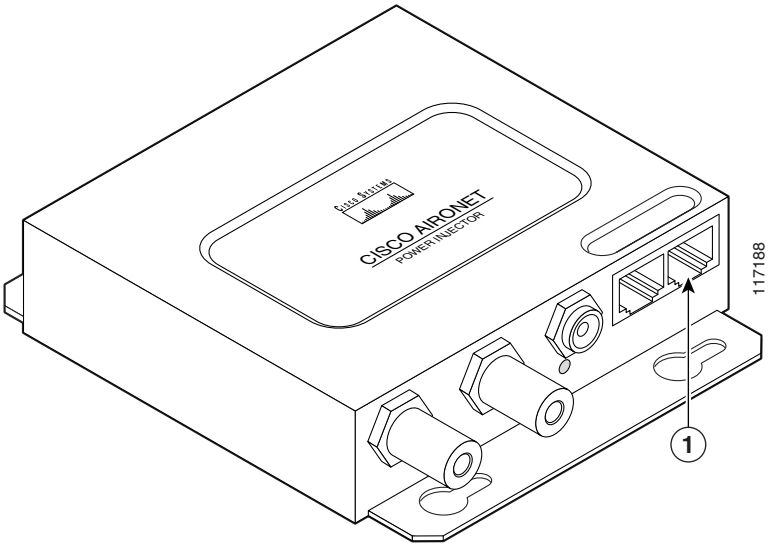
The static information configured with the CLI commands are used by the lightweight access point to connect with a controller. After connecting with the controller, the controller reconfigures the access point with new controller settings, but the static IP addresses for the access point and the default gateway are not changed.

Connecting to the Console Serial Port

If you need to configure the access point locally (without connecting to a wired LAN), you can connect a PC to the power injector console serial port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the console serial port:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the power injector and to the COM port on your PC. Figure 5-3 shows the power injector's console serial port connector.

Figure 5-3 Console Serial Port Connector



1	Console serial port connector (RJ-45 connector)	

Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3 When the terminal emulator is activated, press **Enter**.

Step 4 Enter your username in the User Name field. The default username is *Cisco*.

Step 5 Enter the access point/bridge password in the Password field and press **Enter**. The default password is *Cisco*.

Configuring Controller Information

To manually configure controller information on a new (out-of -the-box) access point using the access point CLI interface, you can use these EXEC mode CLI commands:

lwapp ap ip address <*IP address*> <*subnet mask*>

lwapp ip default-gateway *IP-address*

lwapp controller ip address *IP-address*

lwapp ap hostname *name*

Where *name* is the access point name that displays on the controller.

Note The default (out-of-box) Enable password is *Cisco*.

Clearing Manually Entered Controller Information

When you need to move your access point to a different location in your network, you must clear the manually entered controller information to allow your access point to associate with a different controller.

Note This command requires the controller-configured Enable password to enter the CLI EXEC mode.

To clear or remove the manually entered controller information, you can use these EXEC mode CLI commands:

clear lwapp ap ip address

clear lwapp ip default-gateway

clear lwapp controller ip address

clear lwapp ap hostname

Manually Resetting the Access Point to Defaults

You can manually reset your access point to default settings using this EXEC mode CLI command:

clear lwapp private-config

Note This command requires the controller-configured Enable password to enter the CLI EXEC mode.

Returning the Access Point to Autonomous Mode

You can return a lightweight access point to autonomous mode by loading a Cisco IOS release that supports autonomous mode (such as Cisco IOS Release 12.3(8)JA or earlier). When the access point is associated to a controller, you can use the controller to load the Cisco IOS release.

Using a Controller to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using a controller:

Step 1 Log into the CLI on the controller to which the access point is associated and enter this command:

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

(where:

a) *tftp-server-ip-address* is the IP address of the TFTP server

b) *filename* is the full path and filename of the access point image file, such as D:/Images/*c1310-k9w7-tar.123-8.JA.ta*r

c) *access-point-name* is the name that identifies the access point on the controller.)

Step 2 Wait until the access point completes the reboot.

Step 3 After the access point reboots, reconfigure it using the access point GUI or the CLI. For additional information refer to the *Cisco Aironet 1300 Series Outdoor Access Point Hardware Installation Guide* available at this URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1300 series access point documentation, click **Cisco Aironet 1300 Series** listed under "Wireless LAN Access."

Obtaining the Autonomous Access Point Image File

The autonomous access point image file can be obtained from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/cisco/software/navigator.html

Note To download software from the Cisco.com software center, you must be a registered user. You can register from the web page.

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1300 Series** .

Step 3 Click **Cisco Aironet 1310 Access Point/Bridge**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1310-k9w7-tar.123-11.JA.tar.

Step 8 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 9 On the Security Information window, click **Yes** to display non-secure items.

Step 10 On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.

Step 11 If you checked No, enter the requested information and click **Submit**.

Step 12 Click **Yes** to continue.

Step 13 Click **DOWNLOAD**.

Step 14 Read and accept the terms and conditions of the Software Download Rules.

Step 15 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 16 Click **Save** to download your image file to your hard disk.

Step 17 Select the desired download location on your hard disk and click **Save**.

Translated Safety Warnings

For translated safety warnings, refer to the safety warning document that shipped with your access point or that is available on Cisco.com.

To browse to the document on Cisco.com, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1300 Series** listed under Outdoor Wireless.

Step 3 Click **Install and Upgrade Guides**.

Step 4 Click **Safety Warnings for the Cisco Aironet 1300 Series Outdoor Access Point and Bridge**.

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the 1300 series access point/bridge (model: AIR-BR1310G and AIR-LAP1310G).

This appendix contains the following sections:

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Autonomous Access Point/Bridge Models:

AIR-BR1310G-A-K9-R or
AIR-BR1310G-A-K9

Lightweight Access Point Models:

AIR-LAP1310G-A-K9-R or
AIR-LAP1310G-A-K9

FCC Certification Number:

LDK102052P (AIR-MP21G-A-K9-B-P) or
LDK102052 (AIR-MP21G-A-K9-B)

Manufacturer:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Cisco could void the user's authority to operate this device.

VCCI Statement for Japan

Warning **This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

警告 VCCI 準拠クラスB機器（日本）
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

Industry Canada

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The device is certified to the requirements of RSS-210 for 2.4-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

121403

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC. 121404

This device complies with the EMC requirements (EN 60601-1-2) of the Medical Directive 93/42/EEC.

This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

For the 1300 series access point/bridge, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

The following CE mark is affixed to the 1300 series equipment:

The above CE mark is required as of April 8, 2000 but might change in the future.

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

Note Combinations of power levels and antennas resulting in a radiated power level of above 100 mW eirp are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Cisco Corporate Compliance.

Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements in CFR 47 Sections 2.1091, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The AIR-ANT3338 dish antenna should be installed more than 22 cm from your body or nearby persons. All other antennas should be installed more than 20 cm from your body or nearby persons.

Guidelines for Operating Cisco Aironet Access Points and Bridges in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points in Japan. These guidelines are provided in both Japanese and English.

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-6434-6500

43768

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

   Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Access Points and Bridges in Taiwan

This section provides administrative rules for operating Cisco Aironet access points in Taiwan. The rules are provided in both Chinese and English.

All Access Points and Bridges

Chinese Translation

低功率電波輻射性電機管理辦法

第十四條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

95815

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 17

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-BR1310G-A-K9
AIR-BR1310G-A-K9-R

Regulatory Information

Figure 1-1 contains Brazil regulatory information for the AIR-AP1310G-A-K9 and the AIR-BR1310G-A-K9-R access points.

Figure 1-1 Brazil Regulatory Information

Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

English Translation

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following URL:
http://www.ciscofax.com

Declaration of Conformity Statements for European Union Countries

The Declaration of Conformity statement for the European Union countries is listed below:

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

Product:	***AIR-BR1310 G-E-K9*** *Cisco Aironet 1300 Series 54 Mbps 2.4 GHz Wireless Campus Bridge*
Va riant:	***AIR-BR1310 G-E-K9-R***
Options included:	***AIR-MP21G-E-K9-A*** *2.4 GHz 54 Mbps Mini PCI Radio Module*

Fulfils the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328 v1.4.1: 2003-04**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark: CE 0

Date & Place of Issue: 15 September 2004, San Jose

Signature: **Tony Youssef**
Director Corporate Compliance
Cisco Systems
125 West Tasman Drive
San Jose, CA 95134 - USA

DofC 375906rev1

Access Point Specifications

This appendix provides technical specifications for the access point/bridge, power injector, and power module. Table C-1 lists the technical specifications.

Table C-1 Access Point, Power Injector, and Power Module Specifications

Category	Access Point	Power Injector and Power Module
Size	Integrated antenna configuration: 8.00 in. W x 8.10 in. H 2.62 in. D (20.32 cm W x 20.57 cm H 6.66 cm D)	Power injector: 4.62 in. W x 4.76 in. H x 1.07 in. D (11.74 cm W x 12.09 cm H x 2.72 cm D) Power module: 3.88 in. L x 1.24 in. W x 2.17 in. D (98.5 mm L x 31.4 mm W x 55.0 mm D)
LEDs	Four LEDs on the back panel: Radio (R), Ethernet (E), Status (S), and Install (I).	One bi-color power LED on the side panel
Connectors	Bottom panel (left to right): Power injector dual-coax ports (two F-type connectors) and two reverse-TNC antenna connectors	Side panel (left to right): Two coaxial uplink F-type connectors, 48-VDC power connector, RJ-45 connector for 100BASE-T Ethernet, and a RJ-45 serial console port connector
Operating temperature	–22 to 131°F (–30 to 55°C) Po	wer injector: –22 to 131°F (–30 to 55°C) Power module: 32 to 104°F (0 to 40°C)
Non-operational temperature	–40 to 185°F (–40 to 85°C) Po	wer injector: –40 to 185°F (–40 to 85°C)) Power module: –40 to 185°F (–40 to 85°C) (10,000 ft. limit)
Humidity	0 to 90% (condensing)	Power injector: 0 to 90% (non-condensing) Power module: 0 to 95% (non-condensing)

Table C-1 Access Point, Power Injector, and Power Module Specifications (continued)

Category	Access Point	Power Injector and Power Module
Operational vibration	SAE J1455	Power injector—SAE J1455
Non-operational vibration	SAE J1455	Power injector—SAE J1455
Environmental testing compliance	The enclosure has been successfully tested and is in compliance with a NEMA 4 enclosure rating.	—
Weight	2.5 lbs (1.13 kg)	Power injector—0.8 lbs (0.36 kg) Power module—1.0 lbs (0.5 kg)
Input voltage	48 VDC (nominal) 53 VDC (maximum)	Power injector (nominal): 48 VDC (LR2 power injector) 12 to 40 VDC (LR2T power injector) Power module: 100 to 240 VAC
Power consumption	13W (typical)	—
Radio output power	For autonomous access points/bridges: 100, 50, 30, 20, 10, 5, or 1 mW (at 1, 2, 5.5, and 11 Mbps) 30, 20, 10, 5, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) For lightweight access points: 100, 50, 25, 12, 6, 3, 2, or 1 mW (at 1, 2, 5.5, and 11 Mbps) 30, 15, 8, 4, 2, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) (Depending on the regulatory domain in which the access point/bridge is installed)	Power injector: 18W (maximum at 48 VDC) supplied to the access point/bridge through dual-coax cables Power module: 18W (maximum at 48 VDC)
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point/bridge is installed)	—
Modulation	IEEE 802.11b-compliant radio: Direct Sequence Spread Spectrum (DSSS) Complementary Code Keying (CCK) IEEE 802.11g-compliant radio: Orthogonal Frequency Division Multiplex (OFDM)	—
Subcarrier modulation	CCK (5.5 Mbps and 11 Mbps) BPSK (1 Mbps, 6 Mbps and 9 Mbps) QPSK (2 Mbps, 12 Mbps and 18 Mbps) 16-QAM (24 Mbps and 36 Mbps) 64-QAM (48 Mbps and 54 Mbps)	—

Table C-1 Access Point, Power Injector, and Power Module Specifications (continued)

Category	Access Point	Power Injector and Power Module
Data rates	IEEE 802.11b/g-compliant radio: 1, 2, 5.5 and 11 Mbps 6, 9, 12, 18, 24, 48, and 54 Mbps (Depending on the regulatory domain in which the access point/bridge is installed)	—
Non-overlapping channels	3	—
Antenna	Integrated antenna 13-dBi patch array Some external antennas: 5.2-dBi omnidirectional 12-dBi omnidirectional 9-dBi patch 10-dBi yagi 13.5-dBi yagi 14-dBi sector 21-dBi dish (Depending on the regulatory region)	—
Environmental air space	The access point/bridge and power injector provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the National Electrical Code (NEC) and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1. **Caution** The power module is not tested to UL 2043 and should not be placed in a building's air-handling spaces, such as above suspended ceilings.	
Safety	UL 60950 UL 2043 CSA C22.2 No. 60950 IEC 60950 EN 60950	Power injector: UL 2043 Power injector and power module: UL 60950 CSA C22.2 No. 60950 IEC 60950 EN 60950 **Note** The power injector and power module must be used in an indoor environment.

Table C-1 Access Point, Power Injector, and Power Module Specifications (continued)

Category	Access Point	Power Injector and Power Module
Electromagnetic Compatibility (EMC)	FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 55022 Class B EN 55024 EN 60601-1-2:2001 AS/NZS 3548 Class B VCCI Class B EN 301.489-1 EN 301.489-17	FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 55022 Class B EN 55024
Radio type approvals	FCC Parts 15.247, 15.205, 15.209 FCC Bulletin OET-65C Canada RSS-102, and RSS-210 Japan ARIB-STD-33B Japan ARIB-STD-66 Europe EN 300.328	—

Channels and Maximum Power Levels

For channel and maximum power level settings, refer to the *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges* or the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges* document available on the Cisco Wireless documentation page of Cisco.com.

To browse to the document, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1300 Series** listed under Outdoor Wireless.

Step 3 Click **Install and Upgrade Guides**.

Step 4 Click **Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges**. or **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.

Console Serial Cable Pinouts

This appendix identifies the pinouts for the console serial cable that connects to the power injector's console serial port. The appendix contains the following sections:

Overview

The access point/bridge requires a special serial cable that connects the power injector's console serial port (RJ-45 connector) to your PC's COM port (DB-9 connector). This cable can be purchased from Cisco (part number AIR-CONCAB1200) or can be built using the pinouts in this appendix.

Signals and Pinouts

Use the RJ-45 to DB-9 serial cable to connect the power injector's console serial port to the COM port of your PC running a terminal emulation program.

Note Both the Ethernet and console serial ports use RJ-45 connectors. Be careful to avoid accidently connecting the serial cable to the Ethernet port connector.

Table E-1 lists the signals and pinouts for the RJ-45 to DB-9 serial cable.

Table E-1 Signals and Pinouts for a RJ-45 to DB-9 Serial Cable

RJ-45 Connector		DB-9 Connector	
Pins	**Signals**	**Pins**	**Signals**
1	NC[1]	–	–
2	NC[1]	–	–
3	TXD[2]	2	RXD[4]
4	GND[3]	5	GND[3]
5	GND[3]	5	GND[3]
6	RXD[4]	3	TXD[2]
7	NC[1]	–	–
8	NC[1]	–	–

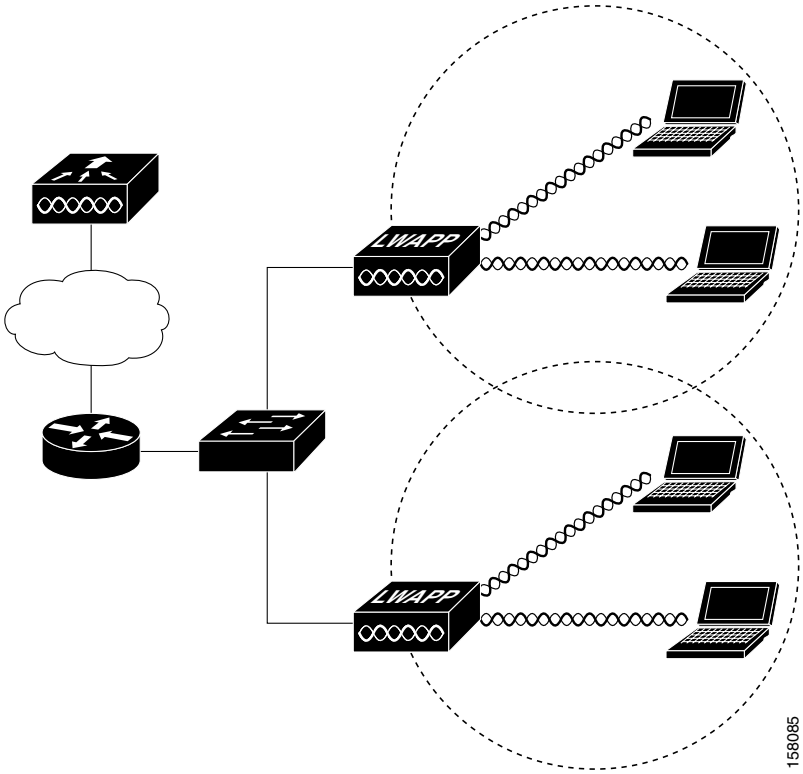
1. NC indicates not connected.
2. TXD indicates transmit data.
3. GND indicates ground.
4. RXD indicates receive data.

Priming Lightweight Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your lightweight access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This helps limit potential installation problems to primarily Ethernet and power areas.

Figure F-1 illustrates a typical priming configuration for your lightweight access points.

Figure F-1 Typical Priming Configuration for Lightweight Access Points



Before deploying your access points to their final locations, follow these steps to prime your access points:

Step 1 In a Layer 2 environment, where the access points are located on the same subnet as the controller, the access point communicates directly with the controller.

Step 2 In a Layer 3 environment, ensure a DHCP server (typically on your switch) is enabled on the same subnet as your access points. The access points will receive its IP address and controller information using DHCP Option 43.

The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the "Configuring DHCP Option 43 for Lightweight Access Points" section on page G-1 for more information.

Note For a Layer 3 access point on a different subnet than the controller, ensure ensure the route to the controller has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure that the routes to the primary, secondary, and tertiary controllers allow IP packet fragments.

Step 3 Ensure that your controller is connected to a switch trunk port.

Step 4 Configure the controller in LWAPP Layer 3 mode and ensure its DS Port is connected to the switch. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate controller guide.

a. In multi-controller environments, You can set one controller's DS port to **Master** (you can use the **config network master-base disable** CLI command or you can use the controller GUI*)* so that new access points always associate with it. You can use the **show network config** CLI command to determine if the controller DS port is the master.

All access points associate to the master controller. From one location, you can configure access point settings, such as primary, secondary, and tertiary controllers. This allows you to redistribute your access points to other controllers on the network.

You can also use a Cisco WCS server to control, configure, and redistribute all your access points from a single location.

Step 5 Apply power to the access points:

a. Connect your access points to untagged access ports on your POE capable switch. You can optionally use power modules or power injectors to power your access points.

b. After you power up the access point, it begins a power-up sequence that you can check by observing the access point LEDs. All LEDs blink sequentially back and forth, indicating that the access point is trying to find a controller.

Note If the access point remains in this mode for more than 5 minutes, the access point is unable to find the master controller. Check the connection between the access point and the controller and ensure they are on the same subnet.

c. If the access point shuts down (all LEDs off), check to ensure that sufficient power is available.

d. When the access point associates with the controller, if the access point code version differs from the controller code version, the access point downloads the operating system code from the controller. All the access point LEDs blink simultaneously during the download.

Step 6 If the operating system download is successful, the access point reboots. Normal operation is indicated when the radio LED is blinking to indicate radio activity.

Step 7 Use the controller CLI, controller GUI, or Cisco WCS to configure the access point with primary, secondary, and tertiary controller names.

Step 8 If the access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.

Step 9 Use the controller CLI, controller GUI, or Cisco WCS to configure the access point-specific 802.11a, 802.11b and 802.11g network settings.

Step 10 If the configuration priming was successful, the radio LED is blinking to indicate normal operation.

Step 11 Repeat Steps 4 to 9 for each access point.

When you successfully complete the configuration priming of all your access points, ensure the Master setting is disabled on your controller. Also you can begin deploying the access points to their final destinations.

Configuring DHCP Option 43 for Lightweight Access Points

This appendix describes the steps needed to configure DHCP Option 43 on a Windows 2003 Enterprise DHCP server, such as a Cisco Catalyst 3750 series switch, for use with Cisco Aironet lightweight access points. This appendix contains these sections:

Overview

This section contains a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with lightweight access points. For other DHCP server implementations, consult their product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

Cisco Aironet 1000 series and 1500 series lightweight access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for Cisco access points capable of operating in lightweight mode are listed in Table G-1:

Table G-1 Lightweight Access Point VCI Strings

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1310
Cisco Aironet 1500 series	Cisco AP LAP1510

The format of the TLV block for 1000, 1130, 1200, 1240 and 1300 series access points is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

Configuring Option 43 for 1000 and 1500 Series Lightweight Access Points

To configure DHCP Option 43 for 1000 and 1500 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS command line interface (CLI).

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1000
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 For the 1000 series lightweight access point, add the option 60 line using the following syntax:

```
option 60 ascii "Airespace.AP1200"
```

The quotation marks must be included.

Step 4 For the 1500 series lightweight access point, add the option 60 line using the following syntax:

```
option 60 ascii "Cisco AP.LAP1510"
```

The quotation marks must be included.

Step 5 Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

For example, if you are configuring option 43 using the controller IP addresses 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the Cisco IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

The quotation marks must be included.

Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, and 1300 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1240
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

option 60 ascii "*VCI string***"**

For the *VCI string*, use the value from Table G-1. The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

option 43 hex *<hex string>*

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is listed below:

option 43 hex f1080a7e7e020a7f7f02

Load-Dump Protection for Transportation Vehicles

This appendix describes load-dump protection that is required for autonomous access point/bridge (model: AIR-BR1310G) operation in some transportation vehicles.

Load-Dump Protection

The autonomous access point/bridge can be installed in vehicles such as automobiles, trucks, and buses. Electronic equipment in vehicle environments can be subjected to high-energy voltage transients where the vehicle battery is accidentally disconnected from the alternator charging circuit. In the Society of Automotive Engineers (SAE) standards SAE J1455 and SAE J1211, this voltage transient is referred to as a *load-dump transient*, where the loading of the battery is dumped or removed from the alternator charging circuits. The access point/bridge does not contain built-in load-dump protection.

Note The power injector LR2T must be used in vehicles providing DC power to the power injector.

Some vehicles contain centralized electronics that are designed to suppress the load-dump transient and prevent equipment damage. To protect the bridge in vehicles without built-in load-dump suppression, you must install an external load-dump protection device, such as the IFM-efector EC2015 for nominal 12-VDC operation or the EC2016 for nominal 24-VDC operation. For additional information refer to the following URLs:

http://www.ifmefector.com/ifmus/web/dsfs!EC2015.html

http://www.ifmefector.com/ifmus/web/dsfs!EC2016.html

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.** Statement 1022

Warning **Connect the unit only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards.** Statement 1033

Caution To prevent damage to the access point/bridge or power injector, connect all coax cables from the power injector to the access point/bridge and connect the power jack to the power injector before applying power.

The external load-dump protection device must be installed across the access point/bridge power cable between the vehicle battery and the access point/bridge. Ensure that the wire size (gauge) is large enough to provide a minimum of 10 VDC to the power injector at all vehicle operating temperatures.

For vehicle cable selection criteria, refer to ISO 6722 (Road Vehicles, 60 V and 600 V Single-core Cables; Dimensions, Test Methods and Requirements).

Numeric

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.

802.11g The IEEE standard that specifies carrier sense media access control and physical layer specifications for 6-, 9-, 12-, 18-, 24-, 36-, 48-, and 54-Mbps wireless LANs operating in the 2.4-GHz frequency band. This standard is also backward compatible with the IEEE 802.11 and IEEE 802.11b standards.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without access points.

antenna gain The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.

associated A station is configured properly to allow it to wirelessly communicate with an access point.

B

beacon A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

bridge A wireless LAN transceiver that is used to connect two or more wired Ethernet networks.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

cell The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.

client A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

dBm An absolute power level described in decibels referenced to 1 mW. 0 dBm is equivalent to 1 mW.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

IP Address The Internet Protocol (IP) address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

isotropic An antenna that radiates its signal in a spherical pattern.

M

MAC Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

N

non-root bridge A wireless transceiver connected to a remote Ethernet network that communicates only with another wireless transceiver connected to the main Ethernet network.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant and IEEE 802.11g-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

P

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

POST Power on self test. A series of diagnostic tests that run during a power up sequence.

power injector A device that supplies DC power to another device over Ethernet communication lines.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

root bridge A wireless transceiver connected to the main Ethernet network that communicates with other wireless transceivers connected to remote Ethernet networks.

roaming A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

RSSI Receive signal strength indicator. A measurement used to help align two antennas for the strongest received signals.

S

spread spectrum A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

transmit power The power level of radio transmission.

U

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

UNII-1 Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

W

WEP Wired Equivalent Privacy. An optional security mechanism defined within the IEEE 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

workstation A computing device with an installed client adapter.

INDEX

R

S

T

U

V

W